

Risky business

**How to develop a skilled
cybersecurity team**

**A remedial approach to destructive
IoT hacks**

**Zero trust: Bringing security up to
speed for the “work-from-anywhere”
age**

New cyberthreats are coming. Prepare today to prevent disaster tomorrow.

- ✓ Effectively prevent against zero-day malware and fileless attacks
- ✓ Intercept email-borne threats before they reach clients
- ✓ Automate your backup and recovery processes, and restore only clean data

A successful cyberattack against a client can lead to data leaks, data loss, and costly downtime — before you even have a chance to react. Stay one step ahead of cyberthreats and reduce client risk with an integrated approach to cyber protection.

Trusted cybersecurity and the best backup
for complete cyber protection



Table of contents

PAGE 04	How to develop a skilled cybersecurity team	PAGE 32	What is the HIPAA Security Rule? Three safeguards to have in place
PAGE 08	Securing your WordPress website against ransomware attacks	PAGE 35	INDUSTRY NEWS
PAGE 11	The warning signs of burnout and how to deal with it	PAGE 42	Why automated pentesting won't fix the cybersecurity skills gap
PAGE 14	How to prevent corporate credentials ending up on the dark web	PAGE 45	What are the post-pandemic security concerns for IT pros and their organizations?
PAGE 19	SECURITY WORLD	PAGE 48	Vulnerability management is facing three core problems: Here's how to solve them
PAGE 24	Risky business: Steps for building an effective GRC program	PAGE 51	How building a world class SOC can alleviate security team burnout
PAGE 26	A remedial approach to destructive IoT hacks	PAGE 54	Top tips for preventing SQL injection attacks
PAGE 29	Zero trust: Bringing security up to speed for the "work-from-anywhere" age		

Featured experts

DAN ANCONINA, CISO & Operations Technology Leader, XM Cyber

STEPHEN CAVEY, Chief Evangelist, Ground Labs

DARREN FIELDS, Regional Vice President Cloud Networking EMEA, Citrix

SASCHA GIESE, Head Geek, SolarWinds

JON HENCINSKI, Director of Global Operations, Expel

THOMAS MACKENZIE, CEO, RankedRight

RAZ RAFAELI, CEO, Secret Double Octopus

CHRIS ROULAND, CEO, Phosphorus Cybersecurity

FAIZ SHUJA, Co-founder, SIRP

BRIAN VERMEER, Developer Advocate, Snyk

NING WANG, CEO, Offensive Security

MIKE WELCH, Managing Director of Strategy and Risk, MorganFranklin Consulting

Visit the magazine website and subscribe at www.insecuremag.com

Mirko Zorz

Editor in Chief

press@helpnetsecurity.com

Zeljka Zorz

Managing Editor

press@helpnetsecurity.com

Berislav Kucan

Director of Marketing

bkucan@helpnetsecurity.com



How to develop a skilled cybersecurity team

Zeljka Zorz

Managing Editor, (IN)SECURE Magazine

What skills should aspiring information security workers possess and work on? What certifications can come in handy more than others? What strategies should organizations employ to develop a well-staffed cybersecurity team? Where should they look for talent? What advice do those already working in the field have for those who want to enter it?

(ISC)² wanted to know the answer to these and other questions, so they asked 1,024 infosec professionals and 1,010 cybersecurity job pursuers in the U.S. and Canada.

What do the information security professionals say?

A previous study by the non-profit organization has revealed the many obstacles to putting job seekers

on a path towards a cybersecurity career.

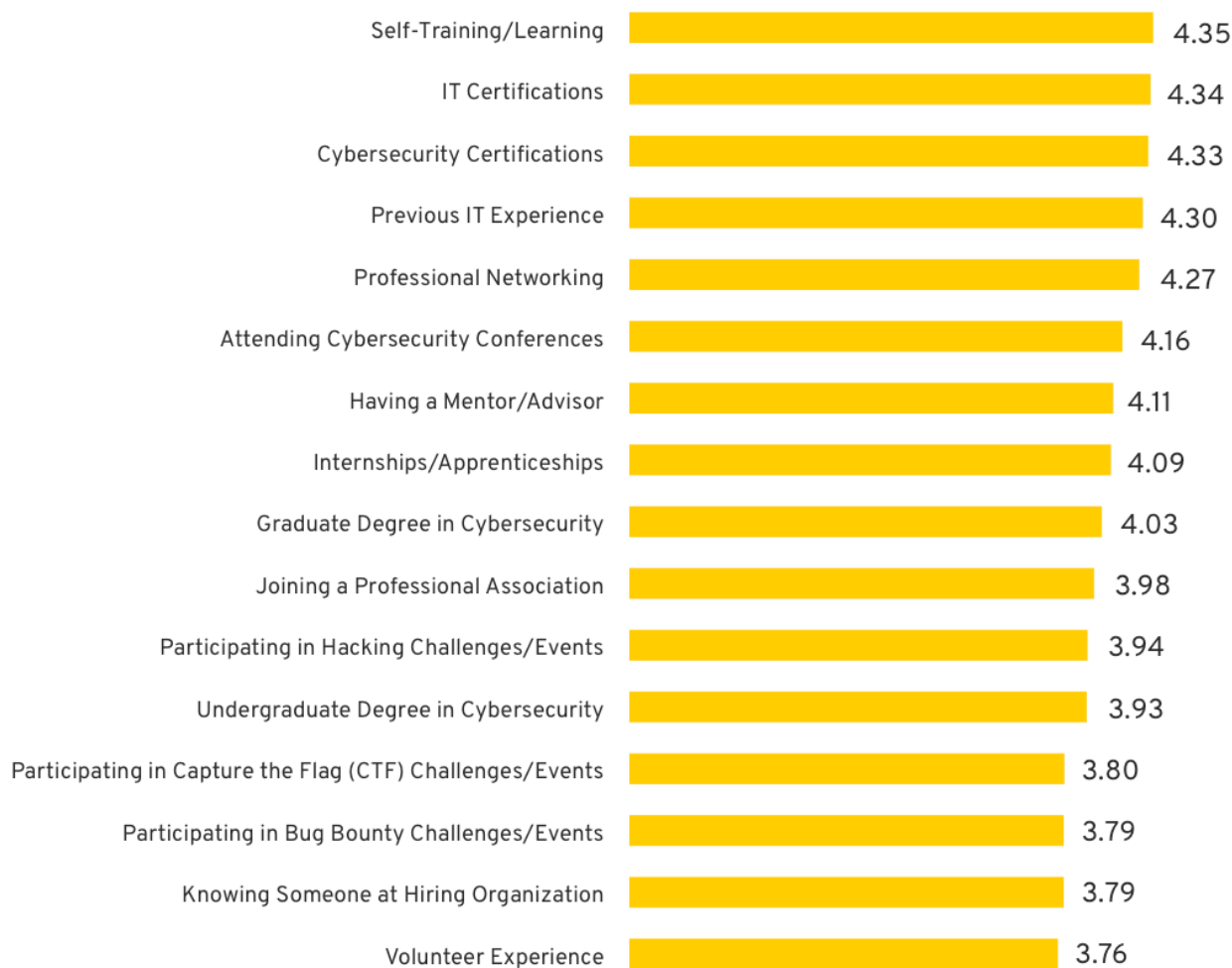
Those who are actively seeking a role in cybersecurity have a pretty good idea which technical skills should they concentrate on acquiring. In fact, that top 5 list is identical to that compiled based on the answers by cybersecurity professionals, and includes cloud security, data analysis, coding / programming, encryption, and

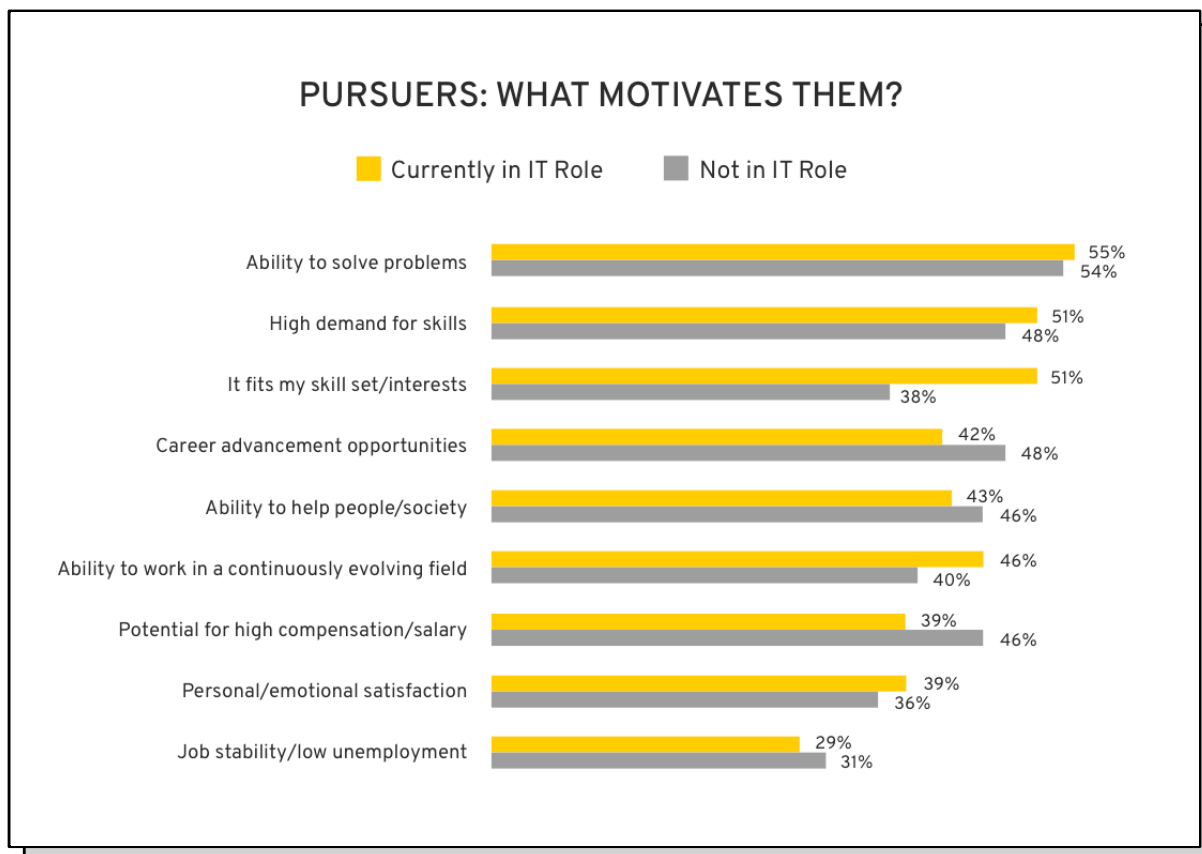
risk assessment / management.

The two groups also have a similar view of what are the most crucial keys to success in cybersecurity are, and those include cybersecurity certifications, IT certifications, and self-training / learning (as well soft skills like problem solving and critical and analytical thinking).

PROFESSIONALS: WHAT'S MOST IMPORTANT FOR PURSUERS?

(Average Rating from 1 to 5)





"Professionals tell us that cybersecurity certifications are important, but they are not necessarily viewed as critical prior to the first years on the job," (ISC)² noted in the recently released Cybersecurity Career Pursuers Study. But later, though, they are a way to prove to employers, their peers and themselves that they possess certain skills.

It's also interesting that, despite cybersecurity pros being more likely to have earned vendor-specific credentials, they think job pursuers should focus more on getting vendor-neutral ones.

Among the other things that allowed them to succeed in the field, they singled out help from mentors, patience and support from the team, and being assigned a project where they could demonstrate their skills and gain self-confidence. On the other hand, common experiences that may have prevented other candidates to thrive include being "thrown into the deep end" and being

overwhelmed with numerous, disparate responsibilities.

"In a field as broad as cybersecurity it may not be a surprise that junior staffers are assigned to such a diverse slate of responsibilities. However, it may suggest a lack of standard, consistent pathways into the field for those taking on their first jobs, as well as unclear routes to advancement and success for many team members," (ISC)² noted.

What do the infosec job seekers say?

Many of the job seekers are confident that cybersecurity is the right career choice for them: they say that they have some of the soft skills required (problem solving), they like to learn new things, they are passionate about cybersecurity, are eager to wrestle with new challenges, and feel that a career in the field can be rewarding. Some also mention job security and good salaries as a draw.

Many of them say that staying current with technology and threat landscape changes will be among the biggest challenges in the first 1-3 years of their cybersecurity career.

Other interesting insights:


- 34% of pursuers with 3 to 6 years of experience in IT show the strongest interest in pursuing cybersecurity jobs
- Women with IT roles seem to show interest in pursuing cybersecurity earlier in their IT careers compared to men
- Most job seekers currently work in the following field: IT services, banking / insurance / finance, and retail / wholesale

"The highest percent of pursuers in our study

currently work in IT services, suggesting this field is fertile ground for new entrants especially among those 35 to 44 years old who may be prime candidates for transitioning to security roles," (ISC)² pointed out.

The non-profit advises organizations to shift from hunting for (increasingly rare) extremely knowledgeable cybersecurity professionals to join their team, and to move towards finding talented and driven people – both in-house and external candidates – and commit to their professional development.

Create realistic job descriptions, seek for diverse candidates (work experience, gender, race, nationality, age), invest in education, foster mentorships, and have patience to see through this long-term strategy, (ISC)² counsels.



helpnetsecurity.com



Securing your WordPress website against ransomware attacks

Jon Hencinski

Director of Global Operations, Expel

It's no surprise to anyone who works in security that there's been an explosion in ransomware incidents over the last two years, costing companies across various industries millions of dollars. According to a recent report from the Institute for Security and Technology, ransomware attacks cost businesses 21 days of downtime, on average.

There are analysts around the globe who are continually being jolted awake in the middle of the night to respond to ransomware attacks. Because WordPress is the market share leader (39.5% of all websites are powered by WordPress; that number jumps to 64.1% for content management systems), my team of SOC analysts aren't strangers to responding to WordPress security issues. The one lesson we've learned time and

time again: Preventative security measures are the most effective steps you can take against ransomware attacks.

For businesses currently on the WordPress platform, we've put together five easy-to-follow tips:

1. Do your homework: Use only the most trusted WordPress plugins

Making sure all plugins on your website are properly vetted and consistently updated minimizes your site's vulnerabilities.

The selection and installation of WordPress plugins should come with the same third-party risk assessment measures (as should any other technology solution you plan to use). It's important to look beyond the capabilities of the plugin and properly research its developer: Does the plugin come with solid reviews and high ratings? Is the plugin's documentation thorough and does it include a link to the developer's website? How many active installations does it have and when was it last updated? Making sure all plugins on your website are properly vetted and consistently updated minimizes your site's vulnerabilities.

2. Create a WordPress hardening guide to outline security best practices

An effective security plugin will validate website configurations and provide added levels of protection but having a WordPress hardening guide in place lays the foundation for security best practices. Your hardening guide should serve as a playbook for maintaining and updating your website's security measures, with information on everything from user administration rules to guides on installing multi-factor authentication plugins or

changing WordPress URLs.

It's important that the person who manages your WordPress also owns the hardening guide, making sure the steps laid out in the guide are implemented, and that the security or IT team performs regular audits.

An effective security plugin will validate website configurations and provide added levels of protection.

3. Publish a Content Security Policy

In addition to a WordPress hardening guide, publishing a Content Security Policy (CSP) adds an extra layer of protection by establishing a protocol for the JavaScript that can run on a webpage, along with how functionality works across the website. It helps prevent cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks and should be as restrictive as possible. CSPs don't need to be revisited unless your development team adds new features that may be blocked by the existing policy.

A good example of an effective CSP solution is SELinux: Once you make sure the application you're running clears all security checks, you can enable it and only revisit your CSP if a webpage's functionality changes.

4. Use password-protected environments to lock down all staging and development instances

Typically, development and staging instances are kept behind a portal or attached to an obfuscated URL, but mistakes happen. Adding password protections to your staging and development environments ensures they remain locked down and safe from bad actors looking to cause harm, or

even innocent admin users who may unknowingly exploit a vulnerability within your WordPress platform.

Adding password protections to your staging and development environments ensures they remain locked down and safe.

5. Run incident response (IR) tabletop exercises to identify vulnerabilities and refine your recovery plan

An IR tabletop exercise simulating a ransomware attack where your WordPress site is the entry point allows your security team to walk through the necessary actions should an incident happen, and ensures you have answers to crucial questions. For example, who's the contact if you need to engage a

third-party site administrator? How quickly can they respond? An IR tabletop exercise answers these questions and allows your security team to train "muscles" they hopefully won't need to use often.

These five tips are all centered on preventative measures to safeguard your WordPress website. Unfortunately, even the most secure websites that follow all the rules can fall victim to attackers. Should this happen to you, remember that an incident isn't resolved until these two questions are answered:

1. How did the ransomware impact your business?
2. How did it enter your website?

Until you have answers to these two questions and can tell a clear and concise story about what happened, your ransomware attack will remain an open case.

Get serious about password security

S P E C O P S

Specops Password Policy Tools Help Block Over 2 Billion Breached Passwords

Specops Password Policy extends the functionality of Group Policy and simplifies the management of fine-grained password policies. The solution can target any GPO level, group, user, or computer with customized dictionary and passphrase settings.

- Block over 2B breached passwords from our collected database that's updated in real time
- Utilize dynamic feedback for end-user password change
- Length-based password expiration with customizable email notifications, & more
- Enforce compliance requirements like NIST, SANS, and PCI

bit.ly/specops-software





The warning signs of burnout and how to deal with it

Thomas Mackenzie

CEO, RankedRight

It's easy for information security professionals to feel burnt out. From the constant stream of security alerts to the demands of senior management, it can be tempting for your team to throw up their hands and say "Enough!"

The consequences of such an action could prove dire for your business, though, so before you let another day of stress go by, read on to learn some warning signs and tips on how to deal with burnout. The goal is to get your team working at maximum capacity without overworking them.

Signs of burnout

Burnout is the word used to describe acute exhaustion when your work becomes overwhelming and too stressful. It can lead to poor

performance, absenteeism, or resignations. It is a real problem in many industries, but it's hugely prevalent in information security because of the long hours and high pressure.

Fortunately, burnout comes with early warning signs that you can spot and address. These include:

1. Anger at colleagues
2. A constant feeling of exhaustion that could manifest in team members getting lost in daydreams or even nodding off at their desk
3. Expressions of hopelessness or being overwhelmed by their responsibilities or current task
4. The team member isolating themselves from others, i.e., avoiding time out with colleagues or social events
5. Unhappiness in the role
6. An inability to stop and take breaks
7. An increase in working hours (coming in early, staying late, skipping lunch, or frequently emailing during out-of-office hours)

If any of your staff shows some of these symptoms, it's time to act!

Taking steps to head off burnout

The first step is to try and understand the cause of the pressure. In many cases it will be a lack of control over one's own workload, but there also may be external reasons for the team feeling exhausted (e.g., unsupportive management, unrealistic expectations).

Get some one-on-one time with the team members to check in on their workload and state of mind. By

The first step is to try and understand the cause of the pressure.

meeting with every team member, it won't look like you're singling anyone out and you can identify patterns in the responses.

- Have there been any resource changes recently?
- Have targets been increased?
- Is management paying closer attention to the team's output?
- Perhaps there are too many meetings?

All these things could be having an effect.

Taking regular breaks to recharge one's batteries can do wonders for mental health as well as productivity.

Once you have a clear understanding of the situation, you can devise a plan for tackling the impending burnout in your team.

The first action would be to work with them to reset expectations – both management's and their own. If they can see that what they should be aiming for is realistic after all, the pressure should be eased, and they'll regain a feeling of control. Things should then start to return to normal quickly.

Another key step is to reintroduce a better work/rest balance across the team, making breaks and hour-long lunches (away from the desk) mandatory - if needed. Taking regular breaks to recharge one's batteries can do wonders for mental health as well as productivity.

That break could be spent taking a walk outside, grabbing lunch with co-workers or even just shutting down for the day when it's clear that no more work can be accomplished in a single shift. And the best way to enforce this work/rest balance is to show that you, as management, are doing it too.

If the workload and expectations on the team cannot be changed, then recruitment or upskilling may be required.

You could go a step further and encourage the team to take up a new activity to support their mental health and wellbeing. This could be a little exercise in the morning before work starts or trying a new hobby.

If the workload and expectations on the team cannot be changed, then recruitment or upskilling may be required. Investing in training and coaching for your employees will help them to feel appreciated and become more productive.

If the budget doesn't allow for an increased headcount, perhaps investing in technology to automate some of the team's most time-consuming processes could be the answer.

Likewise, new blood in the department could give the team the extra support and energy boost they need. Keep in mind, though, that there's currently a major information security skills shortage, so if you're lucky enough to find more worthy candidates than you need, keep in touch with those you couldn't hire because they may become useful soon.

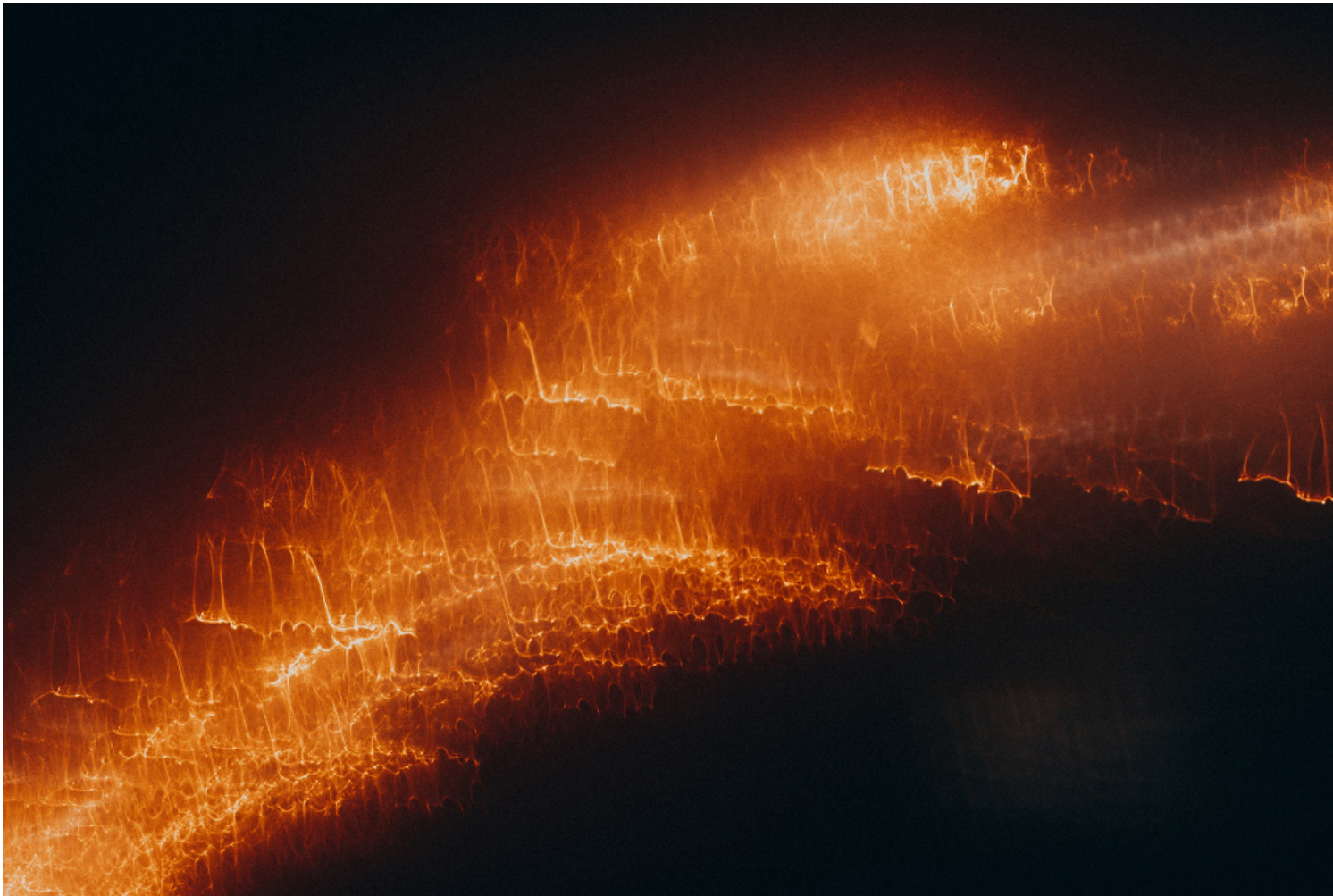
It is possible to maintain a healthy balance in your team while still getting the work done.

If the budget doesn't allow for an increased headcount, perhaps investing in technology to automate some of the team's most time-consuming processes could be the answer. One such task is the daily prioritization of new vulnerabilities picked by your scanners. This can be easily automated to help your team focus on the critical work of remediation.

If burnout is imminent – i.e., it's too late for the above steps - it might be wise to offer counselling services to the affected team members. This can take the form of one-on-one sessions or access to meditation apps or online programs.

If burnout is imminent – i.e., it's too late for the above steps - it might be wise to offer counselling services to the affected team members.

It is possible to maintain a healthy balance in your team while still getting the work done. All you need to do is be aware of how things are going and make sure that everyone has time for themselves, too. Remember that it can take some people longer than others to recover from pressures, so don't ignore these signs before they get worse!



How to prevent corporate credentials ending up on the dark web

Raz Rafaeli

CEO, Secret Double Octopus

A little over \$3,000 — that's how much stolen corporate network credentials tend to go for on the dark web. Although the exact asking price for an individual's credentials may depend on several factors, like how much revenue their enterprise makes, particularly valuable organizations may even see their login details auctioned off for as much as \$120,000. While a successful ransomware attack is capable of fetching cybercriminals almost 10 times as much in ransom, even expensive credentials can be money well spent.

Unfortunately for enterprises, the consequences of corporate credential exposure on the dark web are not just limited to direct financial loss. Ease of access to company login details may also lead to (among other things) a damaged company

With a rising incidence rate of advanced persistent threats that can move laterally within infected networks, a single employee's credentials can be enough for a threat actor to wreak havoc across an entire organization.

reputation, loss of intellectual property, and increased insurance premiums.

With a rising incidence rate of advanced persistent threats that can move laterally within infected networks, a single employee's credentials can be enough for a threat actor to wreak havoc across an entire organization.

The number of exposed corporate credentials continues to rise

Last year saw a 429% increase in the number of corporate login details with plaintext passwords exposed on the dark web. This dramatically increased rate of exposure means that an average organization is now likely to have 17 sets of login details available on the dark web for malicious actors to exploit.

It's not just small and medium-sized enterprises with poor cybersecurity that are seeing their credentials shared on hacker forums. This year, SpyCloud found almost 26 million Fortune 1000 business accounts and 543 million employee credentials circulating on the dark web, a 29% increase from 2020.

Even companies that are supposed to be on the front line of cyber defense are overexposed to this threat vector. A staggering 97% of cybersecurity companies have had their data leaked on the dark web.

6 ways to keep corporate credentials safe

Luckily, organizations are not totally helpless when it comes to its passwords being put up for sale on the dark web. Below are six steps every business can and should take to ensure their corporate credentials remain secure.

1. Use unique passwords for all accounts and systems

The first step in keeping any organization safe is communicating to employees the importance of using different passwords for different accounts and systems.

Cybersecurity professionals have been warning companies about the necessity of strong, unique passwords for decades. Yet, despite plenty of warnings, password reuse remains common practice. The average employee is likely to reuse the same password about 13 times. Even worse, 29% of stolen passwords are weak. For example, the SpyCloud Breach Exposure Report discovered that Fortune 1000 employees were no strangers to using passwords like 123456789, (companyname), and Password.

Cybersecurity professionals have been warning companies about the necessity of strong, unique passwords for decades.

At the very least, organizations should ban the use of these "bad passwords".

However, seeing how workers manage too many passwords to make each a unique one and still remember them all, expecting employees to do so is not exactly realistic. One way you can encourage workers to create unique passwords is to give

them access to a password manager.

By allowing employees to use a password manager for personal use as well, you will significantly reduce the likelihood that they'll reuse the same password across different applications. This approach is made even more crucial as 73% of employees duplicate their passwords in personal and work accounts. It's all too easy for a hacker to gain access to an employee's Netflix account one day and breach their employer's corporate network the next.

2. Replace all passwords regularly

Even if your employees do everything right when it comes to passwords, your organization's corporate credentials could still appear on the dark web. According to a survey by the Ponemon Institute, 53% of companies experienced at least one data breach as a result of compromised third-parties in the last two years.

Changing passwords regularly (every few months or so) can help ensure that even if your organization's corporate credentials appear on the dark web, they will no longer be "fresh" and, therefore, less useful to cybercriminals.

MFA adds an extra layer of protection, making it much more difficult for cybercriminals to log in as someone else.

3. Enable multi-factor authentication

According to Microsoft, most account takeover attacks can be blocked with multi-factor authentication (MFA).

MFA adds an extra layer of protection, making it much more difficult for cybercriminals to log in as

someone else. Unless a malicious actor manages to access an employee's phone, email, or USB in addition to gaining access to their password, they won't be able to log into their corporate accounts or systems.

However, keep in mind that MFA, especially SMS MFA, is not foolproof. Hackers have tools to spoof, intercept, and phish SMS.

Educating employees on cyber threats and how to spot them is crucial to mitigating attacks.

4. Provide safety awareness training to employees

Employees are the weakest link in any organization's security posture. A Tessian report found that 43% of US and UK employees have made mistakes that resulted in cybersecurity repercussions for their organizations. Phishing scams, including emails that try to trick employees into sharing corporate login details, are particularly common.

Educating employees on cyber threats and how to spot them is crucial to mitigating attacks. However, for training to be effective, it needs to consist of more than just repetitive lectures.

In the report mentioned above, 43% of respondents said a legitimate-looking email was the reason they fell for a phishing scam, while 41% of employees said they were fooled because the email looked like it came from higher up. Live-fire security drills can help employees familiarize themselves with real-world phishing attacks and other password hacks.

Safety awareness training should also teach

workers the importance of good practices like using a virtual private network (VPN) when working from home and making social media accounts private. Discouraging oversharing online is equally as important. More often than not, hackers can get all the information they need to craft a convincing phishing email by scrolling through someone's social media.

5. Monitor the dark web

If you suspect that your organization's corporate credentials have been exposed on the dark web, you can run a dark web scan. There are many tools that enable you to do so, many of which are free. For example, WatchGuard lets you check if your company's assets are in danger at no cost.

That said, you shouldn't search the dark web just once. Data breaches happen all the time, so you need to monitor the dark web continuously. To save time, consider investing in dark web monitoring software.

Dark web monitoring tools scan the dark web on your behalf, notifying you as soon as they come across any compromised credentials for sale that belong to your company. Dark web alerts should give you enough time to act before threat actors use your organization's login details for malicious purposes.

What makes passwordless authentication more secure is that users don't have to enter a password or any other memorized secret to log in to an application or IT system.

6. The holy grail — go passwordless

With 80% of hacking-related breaches caused by

compromised credentials, it makes no sense to rely on passwords. Instead, many businesses are turning to passwordless authentication. In a recent LastPass survey, 92% of organizations said that passwordless authentication is the future.

What makes passwordless authentication more secure is that users don't have to enter a password or any other memorized secret to log in to an application or IT system. Instead, users can prove their identity based on either a "possession factor" (such as a hardware token or a one-time password generator) or an "inherent factor" (like a fingerprint).

Unsurprisingly, 64% of cybersecurity professionals say user experience is the reason their organization is eliminating passwords.

Not only can going passwordless strengthen an organization's security, but it can also improve the user experience. In its "Passwordless Future Report," Okta discovered that almost 50% of users feel annoyed by passwords. In addition, about one in five employees experience delays in their work due to forgotten passwords, and more than one in three employees are frequently locked out of their accounts completely. Unsurprisingly, 64% of cybersecurity professionals say user experience is the reason their organization is eliminating passwords.

Other benefits of going passwordless include a lower total cost of ownership (reducing support ticket numbers) and better visibility over identity and access management.

Get the Ultimate SaaS Security Posture Management (SSPM) Checklist

Cloud security is the umbrella that holds within it: IaaS, PaaS and SaaS. Gartner created the SaaS Security Posture Management (SSPM) category and named it in their article as one of the 4 Must-Have Technologies That Made the Gartner Hype Cycle for Cloud Security, 2021.

With enterprises having 1,000 or more employees relying on dozens to hundreds of apps, the need for deep visibility and remediation for SaaS security settings is only getting more critical. The top pain points for SaaS security stem from:

- 1.** Lack of control over the growing SaaS app estate
- 2.** Lack of governance in the lifecycle of SaaS apps
- 3.** Lack of visibility of all the configurations in SaaS app estate
- 4.** Skills gap in ever-evolving, accelerating, complex cloud security
- 5.** Laborious and overwhelming workload to stay on top of hundreds to thousands (to tens of thousands) of settings and permissions.

Effective SSPM solutions come to answer these pains and provide full visibility into the company's SaaS security posture, checking for compliance with industry standards and company policy. As one might expect, not all SSPM solutions are created equal. When comparing SSPM options, there are some key features to look out for.



Free Download

Check out the Ultimate SaaS Security Posture Management (SSPM) Checklist for the critical capabilities to avoid SaaS misconfigurations.



DOWNLOAD NOW

Security world

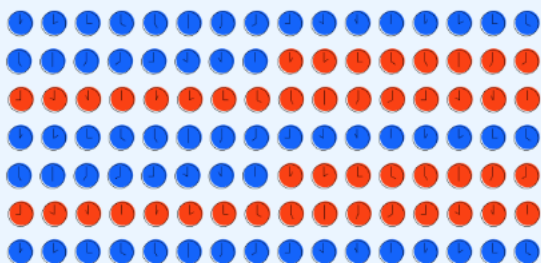
Organizations making security trade-offs in the push to innovate

The vast majority of organizations are increasing their investment in application security this year, but they continue to struggle to fully embrace secure innovation. A market study released by Invicti Security examines how companies are contending with the strategic need to innovate and the existential risk posed by cyber threats.

Tight timelines and innovation pressures for those on the front lines mean skipped security steps. And, integration is still a work in progress: 70% of

respondents “frequently” or “always” complete projects without carrying out all security steps.

Additionally, integration into the software development life cycle (SDLC) is lacking, with only 20% reporting they have fully shifted left and another third in the “messy middle.” The repercussions of this are clear, with one in three issues under remediation making it to production without being caught in the dev or test stages.



112 hours

time it takes **per team member** to address current backlog of security issues

Executives' top concern in Q3 2021? New ransomware models

The threat of “new ransomware models” was the top concern facing executives in the third quarter of 2021, according to Gartner. Concerns about ransomware topped pandemic-related concerns, including supply chain disruptions, according to the survey of 294 senior executives across industry and geography.

“The negative impact of evolving ransomware attacks is seen as so severe by executives that it tops a notable list of risks related to an ongoing pandemic and the disruption of the global supply

chain,” said Matt Shinkman, VP with the Gartner Risk and Audit practice.

The risk of new ransomware models made its debut in the top five emerging risks in the third quarter as the previous quarter’s top risk, “cybersecurity control failures,” has matured into an established risk after consecutive quarters being tracked by the Emerging Risks Monitor Report. The remaining risks in the top five positions were all related to the pandemic and its implications for work.

72% of organizations hit by DNS attacks in the past year

DNS attacks are impacting organizations at worrisome rates. According to a survey from the Neustar International Security Council (NISC) conducted in September 2021, 72% of study participants reported experiencing a DNS attack within the last 12 months.

Among those targeted, 61% have seen multiple attacks and 11% said they have been victimized regularly. While one-third of respondents recovered within minutes, 58% saw their businesses disrupted for more than an hour, and 14% took several hours to recover.

DNS attacks are nothing new, and they tend to fall further down the list of threat concerns.

Ransomware, distributed denial-of-service (DDoS) and targeted hacking of accounts have rounded out the top three perceived threats by NISC survey respondents for the six months beginning March 2021. However, DNS attacks appear to be on a gradual upward trajectory.

In its October 2020 survey, NISC found that 47% of respondents felt DNS compromise was an increasing threat; that number has risen slowly but steadily over the past year and now stands at 55% in the latest release.

According to the survey, 92% of organizations report that their website is vital to business continuity and customer fulfillment at some level, with 16% entirely enabled by it. 56% of respondents consider their website as having a major role in day-to-day activity, while only 8% feel they would be able to conduct business without their website up and running.

Increased risk tolerances are making digital transformation programs vulnerable

Digital transformation programs could be vulnerable to cyber attacks due to increased risk tolerances and ongoing cybersecurity challenges,

according to a global research of 500 cybersecurity decision makers by NCC Group.

Seventy-six per cent admitted that they had increased their risk tolerances to allow changes to their operating model (such as remote working) during the pandemic. Simultaneously, organizations are struggling with security challenges that include balancing proactive security improvements with everyday operations, knowing which risks to prioritise and digesting the volume and complexity of reports from third parties after a security assessment.

How to close the cybersecurity workforce gap

The 2021 (ISC)² Cybersecurity Workforce Study reveals a decrease in the global workforce shortage for the second consecutive year from 3.12 million down to 2.72 million cybersecurity professionals. There are two significant contributing factors to this year's workforce gap estimate. The first is that 700,000 new entrants joined the field since 2020, contributing to a sharp increase in the available supply, now up to 4.19 million people.

The second is that the workforce gap for every region other than Asia-Pacific increased. Data suggests that slower economic recovery from the pandemic and its impact on small businesses and critical sectors like IT services (a major cybersecurity employer in the region) is contributing to the relative softness in demand for cybersecurity professionals compared to North America, Europe and Latin America. However, Asia-Pacific still has the largest regional workforce gap of 1.42 million.

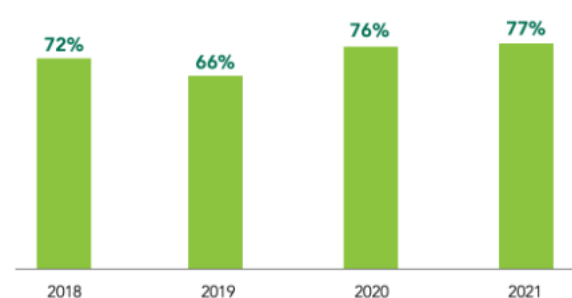
Even with 700,000 new entrants, demand continues to outpace the supply of talent. The

global cybersecurity workforce needs to grow 65% to effectively defend organizations' critical assets.

"Any increase in the global supply of cybersecurity professionals is encouraging, but let's be realistic about what we still need and the urgency of the task before us," said Clar Rosso, CEO, (ISC)².

"The study tells us where talent is needed most and that traditional hiring practices are insufficient. We must put people before technology, invest in their development and embrace remote work as an opportunity. And perhaps most importantly, organizations must adopt meaningful diversity, equity and inclusion practices to meet employee expectations and close the gap."

Strong Job Satisfaction for Cyber Pros
(Satisfied or Extremely Satisfied)



When it comes to collaboration tools, firms struggle to keep up with security and compliance

Surveying 100 key executives across financial services, Theta Lake found that 83% of respondents are turning off key productivity and usability features of collaboration platforms like Zoom, Microsoft Teams, and Webex due to their organizations' technical inability to adhere to relevant regulatory compliance and security

requirements.

Analysis showed that the exponential adoption of collaboration tools since early 2020, coupled with a reliance on legacy archiving and supervision technology built for email, has challenged financial services firms.

Biometrics emerging as the preferred identity verification option for digital consumers

Onfido announced the results of a global study with Okta which revealed that businesses have just 10 minutes to set up digital accounts or risk losing consumer trust.

The significant growth in the adoption of digital services throughout the pandemic has increased customers' confidence in accessing online services. More than half of customers feel more comfortable online than before the pandemic, leading them to ditch shops and in-branch visits in favor of digital convenience.

This rapid shift towards digital services capitalizing on changing consumption models has intensified the customer battleground—and savvy businesses are focused on creating trust in new and improved online products and services.

The survey shows that robust security and a seamless user experience are still non-negotiables

when it comes to building digital trust, and the speed of service has also become essential to the digital consumer when setting up an online account.

The survey showed that companies are “on the clock” the moment that the digital onboarding process begins—with customers expecting it to take no longer than 10 minutes. This is true across all industries; 65% want to open a bank account in less than 10 minutes, 69% when booking a car rental, 72% when opening a telemedicine account and 77% when registering a gaming account.

This need for speed extends to the ongoing service offering. Once onboarded, customers feel that brands should know and trust them, and therefore expect a much quicker authentication process during the customer journey – even for transactions that present a higher risk of fraud to themselves and the company.

Increased activity surrounding stolen data on the dark web

Dark web activity the value of stolen data and cybercriminal behaviors, have dramatically evolved in recent years, according to a Bitglass research. Stolen data has a wider reach and moves more quickly:

- Breach data received over 13,200 views in 2021 vs. 1,100 views in 2015 — a 1,100% increase.
- In 2015, it took 12 days to reach 1,100 link views — in 2021, it took less than 24 hours to

surpass that milestone.

- Breach data was downloaded from entities across 5 different continents.

“We expect that the increasing volume of data breaches as well as more avenues for cybercriminals to monetize exfiltrated data has led to this increased interest and activity surrounding stolen data on the dark web,” said Mike Schuricht, leader of the Bitglass Threat Research Group.

Despite spending millions on bot mitigation, 64% of orgs lost revenue due to bot attacks

A Kasada survey covers the state of bot mitigation exclusively from the perspective of organizations already using anti-bot solutions.

64% of organizations lost 6% or more of their revenue due to bot attacks, and 32% report that their organizations lost 10% or more of revenue within the last 12 months. A quarter of respondents say that on average a single bot attack costs their organization \$500,000 or more, and 44% of respondents say it costs their organization \$250,000 or more.

45% of companies surveyed say bot attacks result in more website downtime at their organizations, and about a third say bot attacks result in brand or reputational damage, reduction in online

conversions, and more frequent data leaks. bot attacks resulted in an increase in operational or logistical bottlenecks.

Researchers found that 77% of companies spent \$250,000 or more on mitigating bot attacks within the past 12 months, while 27% spent in-excess of \$1 million, resulting in a loss of revenue and increased operational costs.

With 80% of executive teams asking about bot attacks within the past 6 months, bot attacks and their effects have become a C-Level concern. As a result, 63% of companies plan to increase their spending on bot prevention over the next 12 months.

Risky business: Steps for building an effective GRC program

Mike Welch

Managing Director of Strategy and Risk,
MorganFranklin Consulting



Organizations across the board are facing governance, risk, and compliance (GRC)-related challenges. This is due to an over-management of GRC programs and the deployment and misconfigurations of GRC technologies.

To ensure organizations are prepared to weather the storm of regulations on the horizon, they need to build a GRC program that is compliant by design. An effective GRC program must be more than focused on security, it also needs to meet privacy, business, and IT requirements.

If you're looking to increase the effectiveness of a GRC program, the following four steps will help you build a blueprint for a successful approach that reduces risk and meets organizational objectives.

Understand the situation

Every GRC program should be tailored to the needs and frameworks of the organization, whether they seek most to comply with industry and privacy regulations or to reduce corporate risk to protect customer data or infrastructure.

The first step is to select an appropriate information security framework to follow, such as NIST CSF, FFIEC CAT, ISO 27001, PCI DSS, HITRUST, CMMC, and others. This framework is then used to define the structure of policies and procedures that help maintain appropriate information security controls and match the organizations objectives.

The framework then becomes the blueprint for building a GRC program to manage risks and reduce vulnerabilities. It also helps the organization allocate resources efficiently and protect valuable assets, while defining and prioritizing tasks that improve security posture over time.

Focus on the risk

Risk is at the center of GRC. An effective GRC program starts with defining the risk appetite, which identifies the most impactful risks an organization faces and develops ways to reduce that risk to a acceptable level.

Organizations invest their resources on the risks that pose the largest operational threat, so they must understand what those risks are to protect themselves. I recommend that organizations take a proactive risk-based decision approach and stop managing security reactively.

The second step is to create a security roadmap that outlines what security programs the organization needs to implement, while also being closely aligned with its business objectives. This roadmap includes existing security programs, as well as noting where those programs need to advance. It should also have the foresight and agility to include technologies that may have not yet been discovered for future use and improvement.

Integrate across departments

A sustainable and effective GRC strategy needs to integrate across the business and align with corporate culture, goals, and processes. Complying with privacy and data regulations is no longer just a checkbox, organizations need to have a GRC program as an umbrella strategy to follow and use to sustain practices over time.

However, successfully creating and managing this program is not solely the role of the CISO and security team, it takes a cross-functional approach from IT to legal and communications, and that rises to board level for input and reporting.

Organizations should also find approaches to efficiently collaborate between departments, while also potentially harnessing tools to minimize manual GRC processes and make risk management, audits, and board presentations easier.

Build for the long-haul

As noted, the purpose of a GRC program is to manage enterprise risk and compliance while helping the business achieve its goals. Too much focus on the first at the expense of the second creates a program that is doomed to failure. GRC programs need to be designed to be usable, sustainable, and scalable.

However, being prepared for the unexpected through a GRC program can reduce the impact of business disruptions caused by cyber-attacks, through integrating business continuity, cybersecurity, and organization resilience. Achieving cyber resilience enables an organization to continue business operations as usual with minimal interruption, even during a seemingly severe attack.

A cyber-resilient business that understands its assets and can quickly respond to threats, minimize the damage, and continue to operate under attack, is a business that can grow with confidence, protect its reputation, and strengthen its customer trust. This is the way of a GRC program that is built to last.



A remedial approach to destructive IoT hacks

Chris Rouland

CEO, Phosphorus Cybersecurity

As of this year, there are more than 10 billion active IoT devices all over the world, many of which are deployed in enterprises.

Keeping those devices secure is of the utmost importance, lest they be a way in for attackers, so it's imperative that organizations institute IoT security practices that remediate vulnerabilities and better protect the network—by identifying and securing every “thing”. The main challenge lies in the fact that most companies aren't aware of the spread of devices connected to its network.

Find and fix every “thing”

Executives often greatly underestimate how much of their network is made up of IoT devices—putting the number at about 1 percent. However, it's

typically 20 percent or higher. In fact, IBM X-Force recently estimated that devices make up 43 percent of the access points on the average organization's network.

Device discovery and inventory are the first step in basic security hygiene - but is often harder than expected.

One reason for this discrepancy is that devices are often being deployed without IT department knowledge or approval, as they are often owned and managed by other teams (e.g., facilities management or physical security teams).

It's critical for companies to get a handle on device inventory now. Device discovery and inventory are the first step in basic security hygiene - but is often harder than expected. Many discovery solutions provide little more information than MAC and IP addresses or use signals that knock over existing devices.

What's needed is enriched data that allows for security teams to act. With greater awareness and complete visibility into every connected device, organizations can create a full inventory of IoT devices with all the information required to maintain them.

According to a recent Positive Technologies report, 15% of IoT devices owners continue to use default passwords. This report also found that just five sets of usernames and passwords gave them access to a great number of IoT devices, including IP cameras, routers, DVRs, and smart washing machines.

Default passwords allow attackers to take over IoT devices as easy access points into the network.

From there, they can use these credentials to move laterally, escalate privileges and eventually gain access to an organization's most critical and sensitive assets.

Many organizations turn to segmentation, a legacy approach to IoT device security, quarantining devices on a separate network and keeping insecure devices away from anything important, but this is no longer enough. Even when on their own, limited segments, insecure devices can still pose a threat through additional vector exposures, such as VLAN hopping malware and other entry techniques.

Default passwords allow attackers to take over IoT devices as easy access points into the network.

Segmentation is a temporary solution, but inoculation and remediation technologies fix problems rather than triaging them - ensuring that IoT devices are compliant with the same policies traditional endpoints are expected to meet for optimal security.

The average timeframe for applying vulnerability patches and rotating credentials is seven years, making them the softest targets on the network today.

The average timeframe for applying vulnerability patches and rotating credentials is seven years, making them the softest targets on the network today. Policy-driven password rotation and implementation of security patches and updates will keep data protected and prevent malicious

actors, like Mirai botnet, from opening the back door.

Automation for security

Automating security is critical to scaling IoT technologies without the need to scale headcount to secure them. To keep up with manual inventory, patching and credential management of just one device it takes 4 man-hours per year.

If an organization has 10,000 devices, that nets out to 40,000 man-hours per year to keep those devices secure. This is an impossible number of working hours unless the business has a staff of 20 dedicated to the cause.

To continuously secure the thousands, or even tens of thousands, of devices on an organization's networks, automation is necessary. With the mass scale of IoT devices and the opportunities to strike in every office and facility, automated identification, and inventory of each device so that security teams can understand how it communicates with other devices, systems and applications, and which people have access to it is crucial.

To continuously secure the thousands, or even tens of thousands, of devices on an organization's networks, automation is necessary.

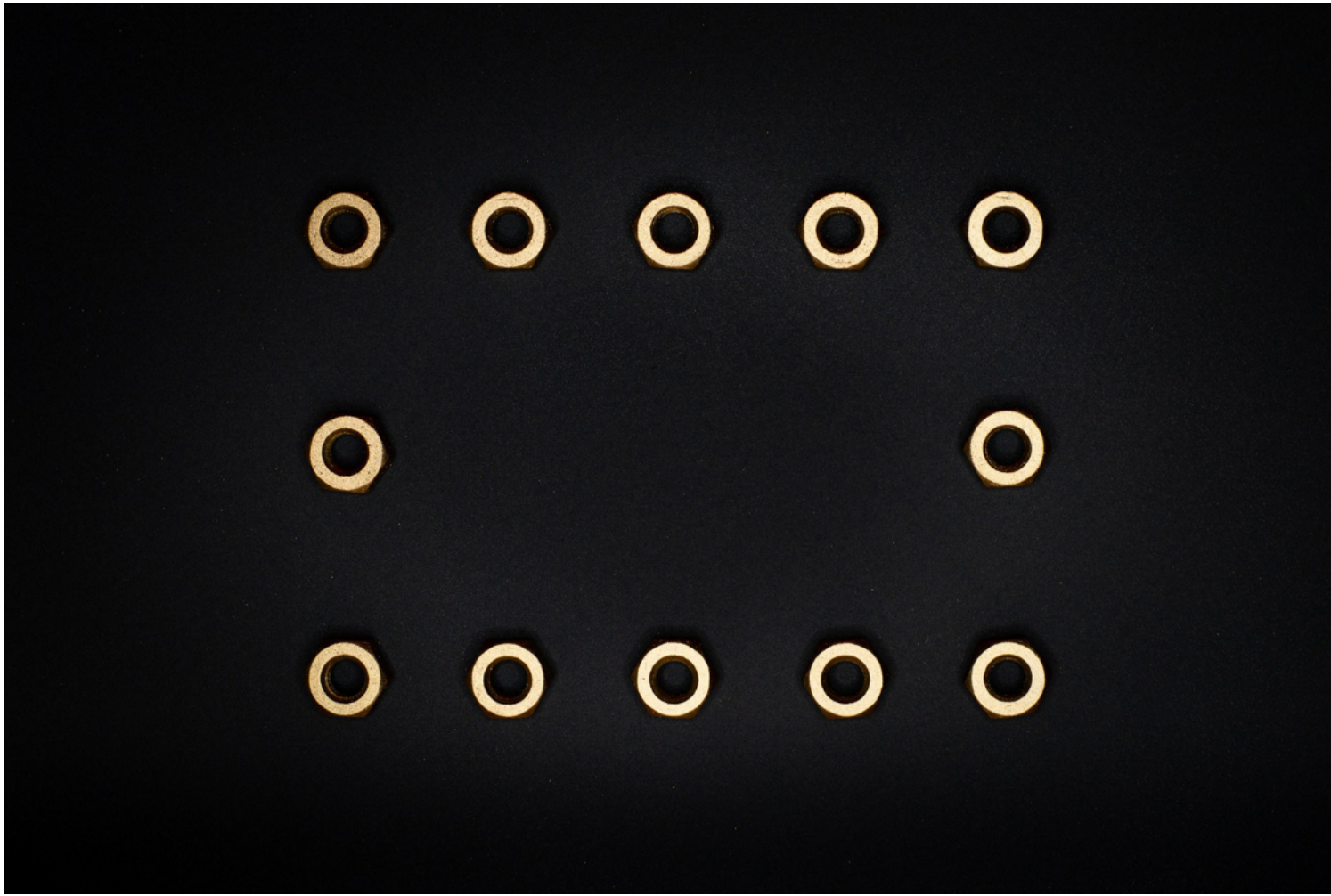
Once identified, automation technology allows for policy compliance and enforcement by patching firmware and updating passwords, defending your IoT as thoroughly as your other endpoints. On top of that, implementing a centralized IoT security tool lets organizations enforce consistent security, better manage IoT devices across their lifecycles and reduce IoT risk.

Organizations invest billions each year on securing desktops, servers, and cloud networks, but by ignoring IoT security their network is vulnerable to attacks. As the attack surface continues to grow, it is now more crucial than ever to install improved IoT security to defend enterprises against cyberattacks and bad actors.



Where do we stand when it comes to multi-cloud maturity?





Zero trust: Bringing security up to speed for the “work-from-anywhere” age

Darren Fields

Regional Vice President Cloud
Networking EMEA,
Citrix

The Internet Age has changed so much of how we live and work. We have become accustomed to buying goods online with a few clicks and having them delivered overnight, and our work lives have become faster, more flexible, and more mobile.

And yet, many businesses still adhere to the ancient “castle and moat” approach of securing their digital business and workforce. It’s high time to bring security architecture into the modern age, and zero trust is designed to enable exactly that.

The (pre-existing) trend toward a more distributed, mobile way of working has been supercharged by the global pandemic. Employees are seeking new approaches that optimize their work-life balance while giving businesses the flexibility required for agile workflows.

Employees are seeking new approaches that optimize their work-life balance while giving businesses the flexibility required for agile workflows.

This shift comes with security challenges. Employees now frequently work outside the traditional security perimeter, use their own devices, as well as a growing number of cloud services instead of – or in addition to – traditional and centrally-managed devices and on-premises business applications. This heterogeneous environment makes it increasingly difficult to achieve the level of control required to keep business processes adequately secured.

Zero trust doesn't mean that businesses no longer trust their employees.

A new security architecture is required. That's why the zero-trust approach is so hotly debated these days. Zero trust doesn't mean that businesses no longer trust their employees. Rather, that they cannot, and should not, have blind faith in the technological context from which employees are accessing sensitive resources.

After all, it is now a likely scenario that employees work with business applications and company data using their own devices and a potentially untrusted network connection like a Wi-Fi home network or public Wi-Fi hot spot. And that's why a zero-trust environment is based on the following concept: "Never trust, always verify."

To achieve this, modern security software, aided by artificial intelligence and continuous monitoring,

constantly evaluates user (or rather: user account) and endpoint behavior for any indicators of unusual activity that might hint at a security compromise.

Not all zero-trust environments are the same, though. In a startup that operates fully based on SaaS, it might be enough to apply the zero-trust concept to SaaS services and endpoint devices.

Most enterprise IT environments, however, are more complex than this: they tend to contain a wide variety of on-premises or even internally developed custom applications, along with legacy VPN technology and a wide array of desktop and mobile devices. Accordingly, the zero-trust approach needs to be carefully planned and adapted to the individual IT environment.

The first step toward a zero-trust environment consists of establishing a zero-trust network architecture that covers all aspects of users interacting with corporate internal and cloud-based IT resources, wherever the users or the resources might be located. This requires an evaluation of the context of user access, combined with the creation of risk profiles.

Based on these risk profiles and continuous context analysis, the security team can implement and enforce centralized security policies – independently from any old-fashioned network firewall perimeter.

Establishing context entails checking numerous aspects such as the IP address and geographic location, device status (corporate-owned, privately owned), OS status (jailbroken/rooted or secure), patch status, and so on, as well as verifying digital certificates for identity and access management.

The constant evaluation of all this data is then matched with predefined granular policies. For

example, businesses might determine that employees can only access sensitive resources if the device is fully secured, and the user is identified via multi-factor authentication. Otherwise, a pop-up notification will inform the employee how to proceed, while the device might be put into quarantine until its desired state is achieved.

The benefit of the zero-trust approach lies in the fact that it strikes a perfect balance between security and usability: most of the time, employees won't even notice that the zero-trust setup is continuously ensuring a high level of security. They will only notice security measures being applied when something extraordinary happens, be it by mistake or because an adversary has managed to compromise a user account.

Business has evolved from the medieval marketplace to just-in-time production, online

Zero trust paves the way for working securely from anywhere while enabling a smooth employee experience.

ordering, and overnight delivery. Similarly, IT security architecture must adapt to today's fast-evolving business world. Zero trust paves the way for working securely from anywhere while enabling a smooth employee experience.

It's high time to leave the ancient castle walls of IT security behind and switch to something designed from the ground up for the speed, agility, and user-friendliness of modern hybrid work.



**DISCOVER WHAT
MATTERS IN THE WORLD OF
INFORMATION SECURITY TODAY**

+ HELPNETSECURITY

helpnetsecurity.com



What is the HIPAA Security Rule?

Three safeguards to have in place

Stephen Cavey

Chief Evangelist, Ground Labs

The past year has catalyzed a new era of healthcare, one where telehealth visits increased as we relied on online communication to keep ourselves informed and healthy. With these adoptions also comes new challenges and considerations, and in this case, more online healthcare data. This influx calls for us to re-examine the HIPAA Security Rule to ensure healthcare entities are protecting patient information.

An introduction to the HIPAA Security Rule

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to improve the efficiency and effectiveness of the US healthcare system as well as patient privacy. In the

following years, several additional rules were added to ensure patients' protected health information (PHI). Two notable rules were added to HIPAA: the Privacy Rule, to help cover the physical security of PHI, and the Security Rule, to safeguard electronic protected health information (ePHI).

In short, the HIPAA Privacy Rule explains what data needs to be protected and who should abide by those rules, whereas the Security Rule was conceived as a national standard to protect patients and explains how to protect ePHI.

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to improve the efficiency and effectiveness of the US healthcare system as well as patient privacy.

The law requires healthcare providers, plans and other entities to uphold patient confidentiality, privacy and security, and calls for three types of safeguards: administrative, physical, and technical.

Administrative safeguards

Covered entities are required to implement administrative safeguards: policies and procedures that describe how the organization intends to protect ePHI and ensure compliance to the Security Rule. Examples include preparing a data backup plan and password management processes (among other things). These standards are laid out in §164.308 of the Security Rule.

These processes include (but are not limited to) implementing the following major standards:

- **Security management:** This includes conducting a HIPAA risk assessment. This risk assessment

most easily be done with a compliance solution provider. A full company scan can reveal gaps and do so more efficiently and thoroughly than a manual assessment. This precaution is mandatory.

- **Security personnel:** Appoint a privacy officer who is responsible for enforcing policies and procedures.

- **Information access management:** Restrict unnecessary access to ePHI. This intersects with physical and technical safeguards. Information access management limits who can monitor and view certain files and its copies, regardless of where it resides (on servers, cloud, etc.)

- **Workplace training and security awareness:** Require employees to complete an annual HIPAA training and educate themselves on their organization's specific security procedures. You may ask why this is so important. While most assume hackers are not present within our organizations, mistakes and human error such as falling for a phishing attack are increasingly common. Arming employees with the knowledge to handle data in a secure manner, identify unusual emails or eliminate insecure habits is crucial to maintaining a strong defense.

- **Contingency plan:** Ensure that processes are in place for unknown future circumstances related to ePHI. This is valuable in the case of an emergency or malicious attack. This rule (§ 164.308(a)(7)(ii)(A)) requires covered entities to "establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information."

Physical safeguards

These safeguards refer to both the physical structure of an organization and its electronic equipment.

Policies and procedures include monitoring and remediating:

- **Access control:** Limit access to facilities that contain computers and servers. This may include implementing procedures that physically protect equipment and facilities from unauthorized personnel. It also means that organizations should have a policy in place to log and keep track of maintenance records and reports that may impact physical security of a premise.

- **Workstation use and security:** Safeguard workstations including any computer, as well as the information within it including controls such as screen saver lock and privacy screen protectors to prevent “eavesdropping”.

- **Device and media controls:** Implement policies for how devices containing ePHI can be removed from a facility if necessary. This rule also requires procedures to be enacted to handle the disposal of hardware that hold ePHI.

Technical safeguards

This component includes the policies and procedures that determine how technology protects ePHI, as well as who controls access to that data. Typically, due to the level of technical literacy needed to understand this regulation, it is the most difficult for entities to understand.

Technical safeguards include the following:

- **Access controls:** Implement technical policies and procedures that allow only authorized persons to access ePHI. This standard also requires individuals to use a unique user identification to view ePHI, have modes in place to allow emergency access, and have technical controls to force automatic log-off after a given amount of inactivity.

- **Audit controls:** Introduce hardware, software, or procedural mechanisms to record and inspect access in information systems that contain or use ePHI.

- **Integrity controls:** Enforce policies and procedures to ensure that ePHI has not been, and will not be, improperly altered or destroyed.

- **Transmission security:** Take technical security measures that guard against unauthorized access to ePHI that is transmitted over an electronic network, this includes a call for encryption.

Safeguard your ePHI

At this time, the US Department of Health and Human Services has hundreds of logged cases of entities who did not protect health information and experienced a data breach, highlighting the severity one mishap can have by impacting hundreds to tens of thousands of patients. Health care information is highly sensitive and needs the utmost protection. The three components of the HIPAA Security Rule may seem difficult to implement and enforce, but with the right partners and procedures, it is feasible.

At this time, the US Department of Health and Human Services has hundreds of logged cases of entities who did not protect health information and experienced a data breach.

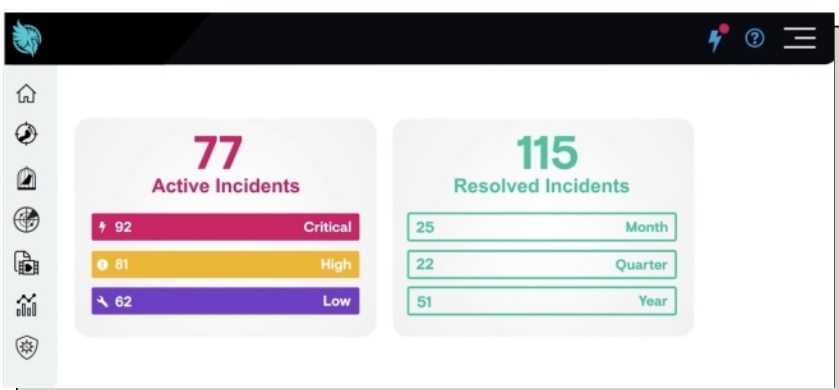
Compliance is never a one-and-done event. You and your organization must take a stance to address compliance on an ongoing basis, as the risks of not doing so are far too great. Beyond the heavy fines and penalties, data breaches can also dissolve patient, customer, and client trust — an even costlier consequence.

Industry news

Huntress launches endpoint protection capabilities to defend SMBs from cyberattacks

Huntress' Managed Antivirus service enables users to extract significant value from Microsoft Defender Antivirus—a built-in and highly capable Windows security tool that's often underutilized. From the Huntress dashboard, users can leverage the service to see detections and events, monitor scans and manage health, set exclusions and execute remediation actions.

"Since Defender is already installed on all modern versions of Windows, installation is as easy as removing any third-party AV on Huntress-managed computers," said Chris Horning, Cloud Services Manager at AtNetPlus. "Defender should just turn itself on and then Huntress begins managing it right away. For MSPs managing thousands of PCs, it really couldn't be easier."



AT&T Managed XDR provides autonomous endpoint threat detection for organizations

The AT&T Managed XDR solution features a cloud-based security platform with security threat analytics, machine learning, and third-party connectors to protect endpoint, network, and cloud assets with automated and orchestrated malware prevention, threat detection, and response.

Through the combination of technologies and 24/7 security monitoring, AT&T Managed XDR helps organizations to detect, respond, and recover faster and at scale from security threats.

Splunk enhances security solutions to help organizations embrace digital transformation

Splunk announced a series of new product innovations designed to help organizations securely embrace digital transformation by providing the security visibility needed to accelerate time to detection, investigation and response.

Led by new enhancements to Splunk Security Cloud and Splunk SOAR, Splunk provides organizations a comprehensive Security Operations Center (SOC) platform with intelligence, analytics and automation.

Enterprise security leaders are in the midst of massive digital transformation, which was further accelerated over the last year due to the scale of remote work and cloud computing adoption. At the same time, organizations are confronted with a continuously evolving threat landscape. Many security products are not designed to integrate with one another, so maintaining end-to-end visibility across on-premise, hybrid and cloud environments can be too complex for security

teams to handle, which leads to blind spots that attackers can exploit.

As a result, SOC's may struggle to quickly detect, investigate and respond to cyberattacks. To address these challenges, Splunk provides an extensive cloud-delivered SOC platform, which is fueled by analytics and driven by automation. With Splunk, organizations can conquer complexity, and defend against threats all the while securely enabling innovation.

"Digital transformation is a top priority for all organizations," said Jane Wong, Vice President of Product Management, Security at Splunk.

"However, many security teams lack visibility across their cloud environments, are overwhelmed by alerts and manual tasks and use too many disparate tools. With Splunk, security teams can detect and respond to threats faster, effectively keeping their organizations more secure in the face of an ever-evolving attack surface."

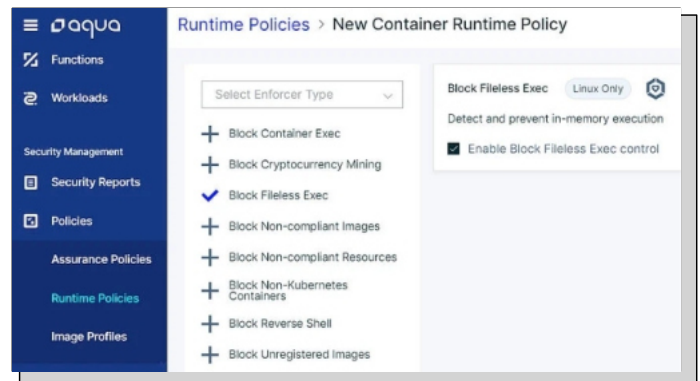


Aqua Security launches CNDR capabilities to detect patterns and respond with granular runtime controls

CNDR leverages continually updated, runtime behavioral indicators that are based on thousands of real-world attacks observed in the wild on cloud native environments, including Linux, Containers, Serverless and Kubernetes workloads. For example, a rootkit tactic that involves loading a malicious kernel, execution of fileless malware, reverse shell, etc.

In addition to behavioral indicators, Aqua's threat intelligence includes IP and DNS reputation intel and a malware database, giving CNDR and Aqua's customers access to the most complete threat intelligence feed for Cloud Native Application security.

"The cloud native threat landscape is constantly evolving. Adversaries are advancing their techniques to craft more sophisticated and

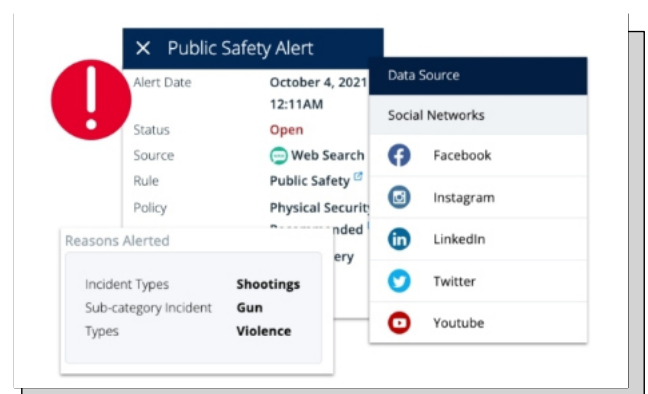


targeted attacks at a rate faster than enterprises can track, which makes the cloud native cyber research performed by Team Nautilus so important," said Amir Jerbi, co-founder and CTO, Aqua Security. "By incorporating the output of this research and intelligence with industry-leading detection capabilities and surgical runtime policies, Aqua delivers the industry's most comprehensive protection for cloud native environments."

ZeroFox Physical Security Intelligence provides real-time situational awareness for security teams

ZeroFox announced a new Physical Security Intelligence solution, delivering visibility and intelligence on supply chain disruption, major events and public safety incidents that may impact worksites, locations, employees, customers and the general public.

The solution delivers high-relevancy alerts on natural disasters, major disruptions and other health and safety concerns. Corporate security teams receive timely, high-fidelity notifications of events that may pose public safety risks to their sites and locations and the people they are protecting.



SecLytics Augur pXDR reduces risk while streamlining SOC operations

Building off SecLytics' patented Augur predictive intelligence technology, Augur pXDR adds core TIP, SIEM, and SOAR functionalities to create a unified, streamlined SOC workflow.

Predictive Intelligence is at the core of everything the Augur pXDR does. The platform starts by using machine learning to model threat actors' behavior and identify attack infrastructure buildup before attacks are launched. Augur correlates that data with threat data from 120 external sources and internal data to build a uniquely customized map of adversaries targeting our clients and their capabilities.

Augur leverages this data to accurately predict future attacks and uses those predictions to automate enforcement across our clients' security

ecosystems. It also uses the data to curate threats that need an analyst's attention, providing enrichment data and visualization to accelerate incident response. Augur also enables orchestrated manual enforcement (blocking and policy updates) across an organization's entire security stack directly from our dashboard.



SecurID Governance and Lifecycle Cloud helps organizations secure the hybrid workforce

SecurID announced innovations that empower security-sensitive organizations to work dynamically, accelerate their cloud journeys and advance zero-trust security with the launch of SecurID Governance and Lifecycle (G&L) Cloud.

Businesses everywhere are grappling with the need to secure hybrid workforces, the accelerating pace of digital transformation, and increasingly complex regulatory environments.

These challenges are exacerbated by ransomware syndicates and other advanced threats that exploit cybersecurity professionals' limited resources and bandwidth, frequently by targeting vulnerabilities in identity and access management and identity governance and administration (IGA). These pressures require new solutions that both deliver immediate business value and advance organizations' long-term strategies.

ReliaQuest releases two capabilities within its XDR platform to improve security operation efficacies

ReliaQuest announced two new capabilities within GreyMatter, its cloud-native open XDR platform: Security Model Index, and Verify. Now with ReliaQuest GreyMatter, organizations can deliver cyber risk metrics, test and validate security controls across their cybersecurity program and take action to continuously improve their risk profile.

“Model Index gives security leaders metrics that provide visibility into performance of their security program, and with Verify, they can be better prepared for the next attack by ensuring their controls are working,” said Brian Foster, Vice President of Product at ReliaQuest. “Now within the ReliaQuest GreyMatter platform, security teams can measure, test and report on the health of their program, and see the specific steps they can take to operationalize these insights to improve their security based on the latest threats and weaknesses in their unique environment.”

Datto SaaS Defense protects cloud-based applications for MSPs

Following its acquisition of Israel-based cyber threat detection company BitDam earlier this year, Datto debuted its SaaS Defense security product built exclusively for MSPs. The advanced threat protection and spam-filtering solution provides MSPs with patented technology to proactively detect and prevent malicious malware, phishing, and Business Email Compromise (BEC) attacks that target Microsoft Exchange, OneDrive, SharePoint, and Teams.

Datto SaaS Defense creates the opportunity for MSPs to attract new clients and expand market share with a robust yet simple security solution that eliminates the need for additional headcount or in-depth security training.



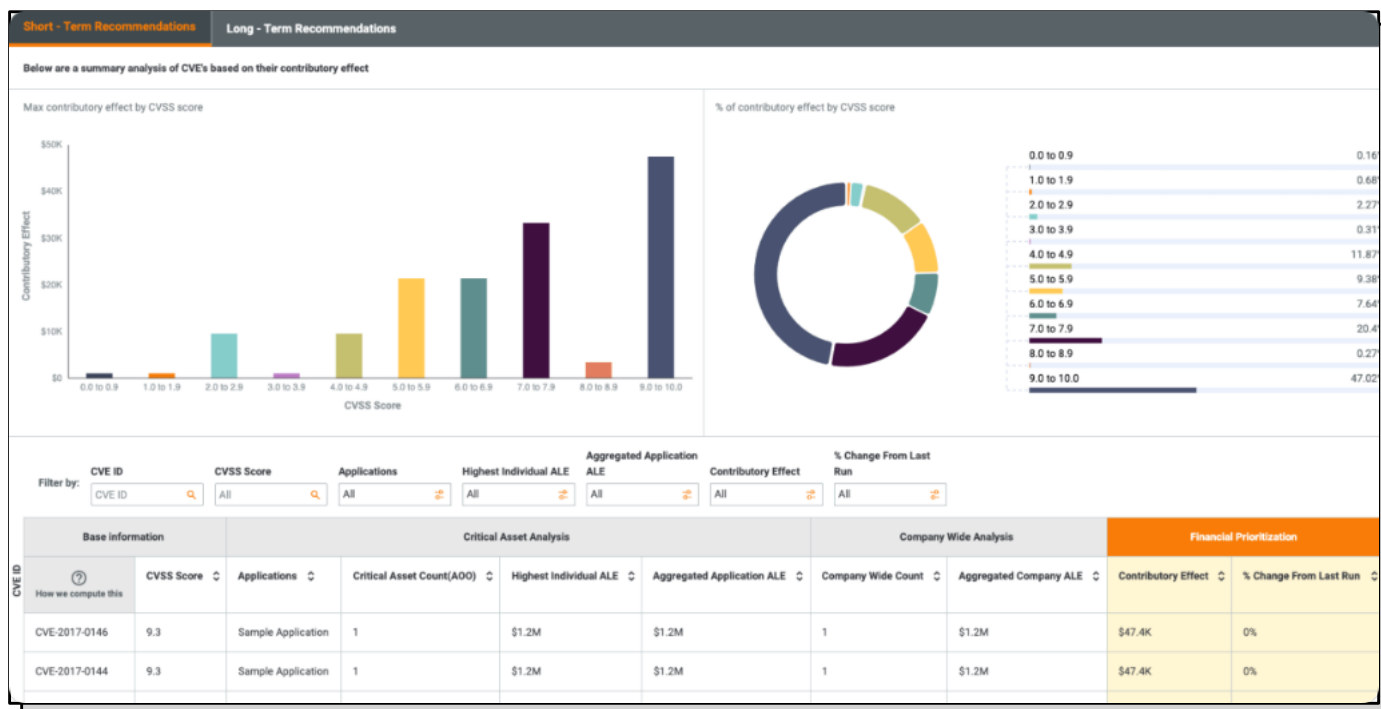
ThreatConnect launches Risk Quantifier 6.0 to bring cyber risk quantification for businesses

ThreatConnect Risk Quantifier (RQ) enables companies to see the financial risks they face from cyber attacks and also prioritize investments that provide the best ROI. RQ's calculations are informed by your internal environment, threat intelligence, vulnerability management, operations and response data found within ThreatConnect and other integrations. RQ is distinctly different from other approaches offered in the market as it focuses on automation and data integration, and delivers value in days and weeks as opposed to months and years.

With RQ 6.0 organizations that are looking at financial cyber risk quantification will have the

option of leveraging full FAIR scenario's, using semi-automated FAIR scenario's, and full automation in one platform.

FAIR is an internationally known standard that has helped companies with awareness and understanding of cyber risk quantification. Organizations implementing FAIR in their CRQ programs have struggled with subjectivity, speed, and actionability, which is why RQ 6.0 is introducing semi-automated FAIR scenario's that automate a large portion of FAIR in order to reduce complexity and increase time to value for customers.



**Your company's
acquisition plans
include
4/*8@Xg>7bS.**

KEEP YOUR BUSINESS — YOUR BUSINESS

Only Echoworx customizable encryption offers you 8 different ways to deliver secure email, support for 27 languages and 7 authentication options. You can easily send email and share information securely from anywhere on any device. Best of all, it's backed by a proven ROI.

Learn more at Echoworx.com

ECHOWORX™
IT PAYS TO BE SECURE



Why automated pentesting won't fix the cybersecurity skills gap

Ning Wang

CEO, Offensive Security

The modern threat landscape is an enormous challenge for the modern enterprise. Many organizations are “addressing” this by buying the newest security products from the latest hot vendor and hoping that this will protect them, but most recognize that this isn't enough to defend their organizations.

Tools and scanners are good to use, but those can only find known vulnerabilities. Many vulnerabilities out there are the kind that only a trained security expert would spot. Unfortunately, the lack of well-trained, qualified security professionals exacerbates organizations' challenges.

The security talent gap is not getting any smaller and people are coming up with some outlandish ideas for closing it. The latest one is automated

penetration testing – the idea is that we can somehow create bots that will probe enterprise defenses and uncover vulnerabilities. Here's the thing though – that's the antithesis of what pentesting is. A real pentest is not an automated scan job. A real pentest leverages the creative mind of an experienced cyber professional.

The security talent gap is not getting any smaller and people are coming up with some outlandish ideas for closing it.

The whole point of pentesting is to be creative, thinking from the perspective of an attacker, and identify vulnerabilities that machines and other pre-built-in logic cannot, thereby staying one step ahead of cybercriminals. When we teach bots to identify and address some vulnerabilities, hackers will get more creative and find new ones to bypass the detection of these automated checks. We should automate as much as we can, but relying only on automated security testing of your systems and networks will not protect your enterprise. The only way to fix this is with great cybersecurity professionals who can beat them to the punch.

Why a shift in mindset is key

Security teams need to have the adversarial or hacker mindset – i.e., they have to think as an attacker. They need to stay a step ahead of the cyber criminals and advise the rest of the organization on the important and timely actions to take.

Not every vulnerability is obvious. The best way to defend the enterprise is for defenders to think like attackers and try harder every time they seemingly hit a dead-end - not giving up easily on something

they see that doesn't make sense. Successfully defending systems, networks, and applications requires not only an understanding of the tools an attacker could use, but how they use them and when they use them. This requires a lot of judgement calls, asking a lot of questions that start with "why", and those cannot be accomplished with automated tests. Automated tests are only as good as what you tell them to look for and do. What makes security hard is that each time, the attacker is doing something different and new.

Attackers don't need a massive vulnerability to impact organizations – they are patient, waiting for an individual to make a mistake to let them in, either via phishing or social engineering. Once in, they make their way up the network or escalate privileges to gain more and more sensitive systems and data.

Automated tests are only as good as what you tell them to look for and do. What makes security hard is that each time, the attacker is doing something different and new.

Bad hacks and data breaches usually start with a small mishap. Because most systems and networks have been designed without necessary security defensive mechanisms, it is not uncommon to chain a few small vulnerabilities to produce a devastating effect.

Moreover, attackers continually develop new malware payloads and test out new threat vectors. The only way to truly level the playing field is with human defenders who are every bit as creative and persistent as the adversaries. The defenders also need to stay up to date on the latest exploits, hacking techniques, malware, etc.

Closing the cybersecurity skills gap

The cybersecurity skills gap is a people problem, but it's not just about finding enough people to operate tools, because the tools themselves are not enough. All tools have a shelf life and it's only a matter of time until attackers find a workaround.

There is no doubt that we need more qualified security professionals and there is no silver bullet to solve this talent shortage.

If we really want to address the security problem, we need to increase security awareness training for all. We need to train people who design and build systems and networks to have an attacker mindset. We must make sure we train the security professionals to have the ability to think like an attacker to stay current with the latest exploits and security issues.

There is no doubt that we need more qualified security professionals and there is no silver bullet to solve this talent shortage. You don't have to be an IT expert to enter the field of security. You need to have a curious mind, be a creative problem solver, willing to put in the sweat to learn the craft, not give up easily and keep going. Great candidates can come from many parts of an organization - system admins, network engineers, web developers, customer support members and even recent graduates. While they won't be able to hit the ground running, they'll have the essential traits to succeed in security.

Security is a people problem. Scanners, tools, and automated tests can help, but to really solve this problem, it takes human creativity on multiple levels to combat it.

HELPNETSECURITY

Follow Us On twitter

Hand holding a smartphone displaying tweets and statistics:

- Help Net Security** @helpnetsecurity · 10h
New standard enhances the cybersecurity of pipeline control systems - helpnetsecurity.com/2021/09/01/pipe... #APIGlobal #scadainfrastructure #SCADA #ICS #cybersecurity #security #infrastructure #helpnetsecurity #securitynews
- Worldwide revenues for managed edge services** will reach \$445.3 million in 2021, an increase of 43.5% over 2020. SOURCE: IDC
- Help Net Security** @helpnetsecurity · 1d
Managed edge services revenues to reach \$445.3 million in 2021 - helpnetsecurity.com/2021/09/01/man... - IDC #OnusianAbout #cybersecurity #security #infrastructure #helpnetsecurity #securitynews #securitynews #market #trending #trends
- Help Net Security** @helpnetsecurity · 1d
Benefits of implementing or expanding a cohesive collaboration solution

63%	50%	43%	40%	40%
Improved productivity	Reduced operational risk	Enhanced security	Increased trust	Enhanced customer experience

 SOURCE: ALCM | FORRESTER

@helpnetsecurity



What are the post-pandemic security concerns for IT pros and their organizations?

Sascha Giese

Head Geek, SolarWinds

COVID-19 has had a huge impact on businesses across every industry, and while the urgent need to adapt in early 2020 may have been replaced with greater stability, residual effects remain. In fact, IT policies implemented to deal with the impact of the pandemic are among the leading macro trends currently influencing enterprise IT risk.

The recent SolarWinds IT Trends Report 2021 found that more than a year of unprecedented upheaval has ultimately served as a catalyst for a wider exploration of the enterprise IT risks currently affecting organizations. External security threats and the risk introduced by a remote and distributed workforce are the most notable, along with cost-cutting and consolidation, but there are plenty of ways IT pros can help their companies deal with the challenges ahead.

Dealing with security breaches

According to the SolarWinds survey, security breaches are seen as the biggest external factor influencing an organization's risk exposure.

46% of the tech pro respondents cited external security threats, such as cyberattacks, as the top macro trend influencing their organizations' risk exposure. So, what can we do to mitigate such threats?

For starters, IT pros need to do everything they can to avoid the apathy and complacency that are sure-fire ways to increase an organization's exposure to risk. It's far too easy to think about security as an add-on that somebody else needs to handle. This can be especially true for IT pros who have been at the same company for a long time or worked at businesses with discrete security teams.

Security falls within every IT pro's responsibility—most of the risks we face are caused by human behavior, and IT pros are very much a part of an extended security team.

IT pros need to do everything they can to avoid the apathy and complacency that are sure-fire ways to increase an organization's exposure to risk.

IT teams need to examine current processes from the outside in and deploy solutions capable of providing complete visibility into all systems to identify areas of risk and opportunity.

Even small changes can make a big difference, such as implementing faster upgrades and patches, or using password managers, and MFA (multi-factor authentication) solutions can easily help strengthen the overall security of a company.

The risk of remote working

External security breaches have coincided with an increase in supporting a remote and hybrid workforce, and 35% of respondents in the SolarWinds IT Trends Report explained the accelerated shift to remote working was the number one aspect of current IT environments considered to increase an organization's risk exposure.

Cyberattacks will likely always be a threat, and security compromises will happen, and this makes it even more important for IT pros to implement detection, monitoring, alerts, and responses along the kill chain, and implementing systems to measure their effectiveness.

The impact of the COVID-19 pandemic has amplified the hybrid IT reality, introducing fragmented policy, configuration, and visibility, increasing the reach of risk from on-premise data centers to the public cloud, IoT, and beyond.

While the shift to remote working was cited as a leading factor in heightened risk exposure for businesses over the past year, and presented a huge challenge during 2020, we've thankfully reached the point where many tech pros are confident with remote work policies.

There are still plenty of things IT pros can do to reduce the level of risk exposure, however. It's critical to move from simply accepting the current exposure to a mindset in which any level of risk exposure is unacceptable.

Cyberattacks will likely always be a threat, and security compromises will happen, and this makes

it even more important for IT pros to implement detection, monitoring, alerts, and responses along the kill chain, and implementing systems to measure their effectiveness.

Other factors contributing to increased risk exposure

Other factors that contributed to an increase in an organization's risk exposure also included a lack of skilled IT staff due to cost-cutting, consolidation, and/or outdated skill sets in employee base (34%).

This is where IT pros may need to step outside their comfort zones, presenting proof points and justifications to senior management to implement more effective policies and technologies at scale.

To win approval and buy-in, recommendations should include facts and figures where possible, pinpointing the impact on customer trust if the

organization chooses to ignore any recommendations. It's also important to highlight other areas of the business that could be affected by security breaches—how much downtime would the business face if there's an unforeseen issue, for example? What's the financial impact on the company, and how does it compare to the cost of investment in a more effective IT security strategy?

Once again, this may seem like it's outside of an IT pro's typical roles and responsibilities, but strategic conversations between IT departments and senior business leaders that can lead to investment where it matters most is imperative to helping cut an organization's risk exposure.

Together, such solutions can help your organization be more prepared to defend against any level of risk exposure, using technology to manage, mitigate, and resolve issues related to risk in 2021 and beyond.

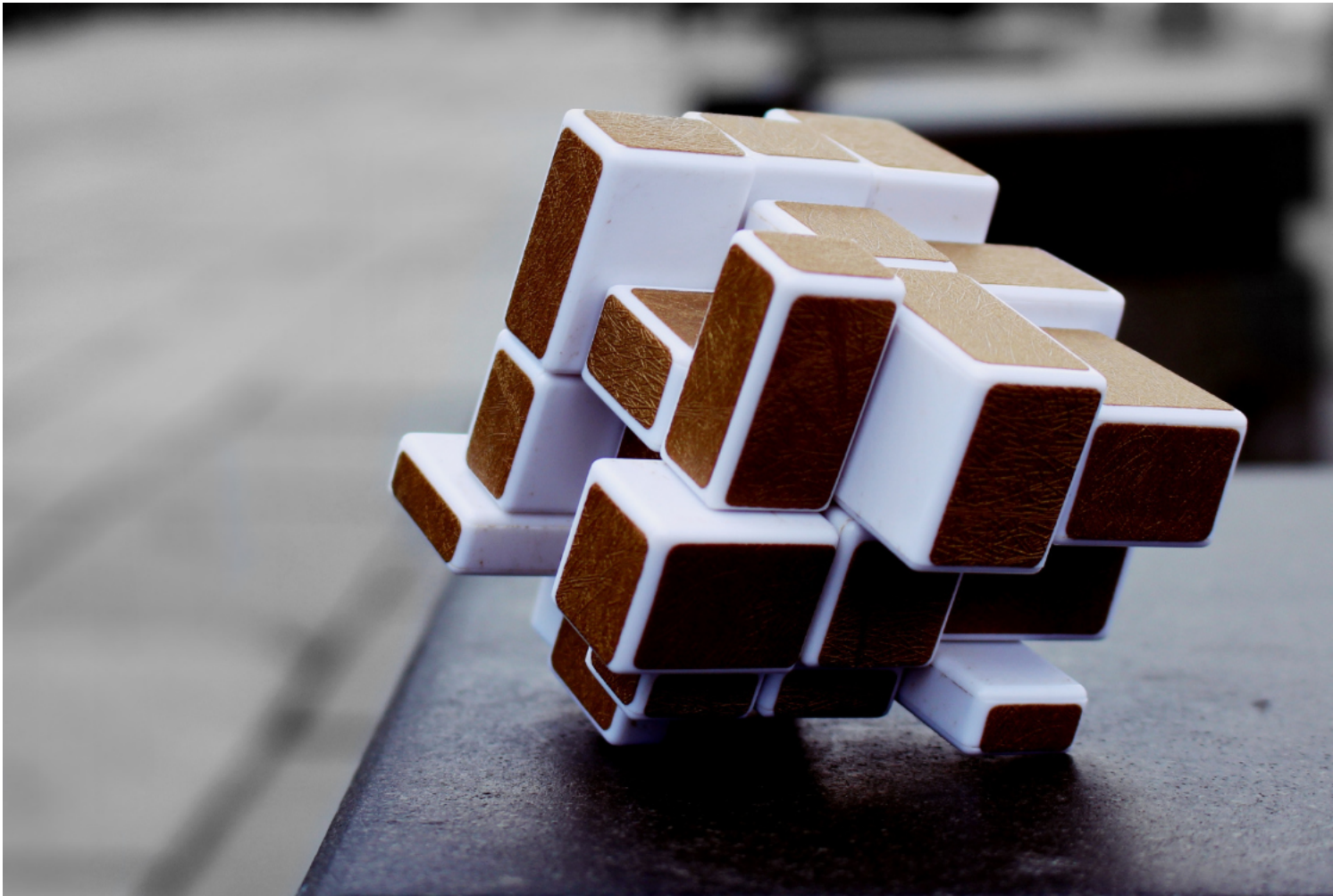


IL IMMERSIVELABS



The Ultimate OWASP Top 10 Cheatsheet

DOWNLOAD NOW



Vulnerability management is facing three core problems: Here's how to solve them

Dan Anconina

CISO & Operations Technology Leader,
XM Cyber

The COVID-19 pandemic has placed enormous stress on information security professionals. A threat landscape that was already growing more complex by the minute now presents an even more fearsome challenge, as cybersecurity budgets are strained, and millions of workers have shifted to telecommuting on a full- or part-time basis.

Where are organizations going wrong in terms of vulnerability management?

From the get-go, too many organizations have an outdated idea of what vulnerability management entails. It's not simply about scanning your networks for threats.

A holistic approach to vulnerability management includes identifying, reporting, assessing and

prioritizing exposures. Crucially, it also involves risk context. Instead of merely scanning for security gaps, a comprehensive approach to vulnerability management shows you how those gaps could be exploited and the consequences that could occur.

It's then accurate to say that vulnerability management - when executed correctly - takes a big picture approach where all aspects work harmoniously to reduce risk to business-critical assets. That is the goal for which we should all strive.

Instead of merely scanning for security gaps, a comprehensive approach to vulnerability management shows you how those gaps could be exploited and the consequences that could occur.

But even if you begin from correct first principles, you can still fail when it comes to implementation. With that in mind, below we've highlighted three of the most significant problems that organizations face when managing vulnerabilities.

Failing to properly prioritize threats

An inability to properly rank exposures is one of the most damaging problems that organizations currently face within the context of vulnerability management. Too many organizations identify security gaps via scanning, then proceed directly to the remediation phase. On some level, that kind of urgency is understandable. Ultimately, however, it is short-sighted and creates more risk.

Smart organizations dedicate plenty of focus to the prioritization and reporting phases of vulnerability management. Failing to prioritize effectively can lead to wasted time and resources,

as teams race to address exposures that pose no real risk to business-critical assets. Even worse, it leaves organizations vulnerable in the worst possible ways. A better way to proceed is to focus on the one percent of exposures that can be exploited. When done correctly, this level of prioritization can eliminate 99-percent of risk to business-sensitive systems.

Failing to prioritize effectively can lead to wasted time and resources, as teams race to address exposures that pose no real risk to business-critical assets.

The best way to benefit from this approach to prioritization? Use a cutting-edge attack path management solution that prioritizes exposures using critical, attack-centric risk context.

A tool that goes beyond limited CVSS scoring and shows the full picture: how likely each vulnerability is to be exploited and the risk each exploit poses to your "crown jewel" assets.

An effective vulnerability management program is ongoing rather than episodic.

Not using a continuous approach

An effective vulnerability management program is ongoing rather than episodic. If enterprises do not take a continuous approach, they will struggle to control the flow of vulnerabilities and build up "vulnerability debt." That's a serious problem.

Given how hard it already is to stay on top of emerging vulnerabilities, working with a continual

backlog of security issues to address can make the entire situation untenable. Instead of irregular scanning and remediation, use an ongoing approach that is centered around continuous and automated vulnerability identification. This is one of the keys to developing a security posture that is defined by continuous improvement.

Poor communication and unclear organizational structure

When security teams do not have clear lines of communication and the right organizational structure problems are almost certain to slip through the cracks.

Too often team members do not have defined roles and they do not understand where they fit within the overall vulnerability management framework, particularly in terms of responsibilities.

When team members have clear roles defined with well-articulated responsibilities, they can work and collaborate effectively. Instead of working in isolation and missing the greater picture, each person can endeavor to meet their responsibilities and achieve their specific objectives - all the while knowing how their work relates to the roles and responsibilities of others.

When team members have clear roles defined with well-articulated responsibilities, they can work and collaborate effectively.

This need for communication extends to the C-suite as well. It's important that the company's leadership understand and are invested in the program, given how strong cybersecurity has become a critical strategic objective.

The takeaway

The consequences of failing to effectively manage cyber vulnerabilities have never been higher. One data breach can lead to crippling reputational and financial damage, and the number of breaches continues to rise, without fail, every year.

Truly, vulnerability management has left the realm of being just another IT expense - it should be a key business objective.

To make that a reality, it's imperative to understand that vulnerability management should be an ongoing, multi-stage process. It's also essential to address the problems that snare so many otherwise smart IT departments: poor prioritization, an episodic approach to managing vulnerabilities and a lack of organization and communication among teams and leaders.

Truly, vulnerability management has left the realm of being just another IT expense - it should be a key business objective.

The right approach can pay massive dividends in terms of avoiding these pitfalls. As mentioned above, the best thing you can do is to incorporate powerful vulnerability management tools that offer proper prioritization guidance and critical risk context.

Once your underlying strategy is sound and you're armed with the right tools, your enterprise will be far ahead of most of your competitors when it comes to protecting your most valuable assets.



How building a world class SOC can alleviate security team burnout

Faiz Shuja

Co-founder, SIRP

For security leaders, building a mature Security Operations Centre is about establishing robust processes that bring teams and technology together for success. Yet many SOC teams are stuck fighting fires without the time, staff, resources, or visibility they need to operate effectively. This situation not only increases the chances of critical alerts being missed, but can quickly foster a stressful, unfulfilling environment that leaves staff burned out and looking for greener pastures.

Recent research indicates that 51 percent of SOC teams feel emotionally overwhelmed by the impossible volume of security alerts they must deal with, with the stress impacting their home lives.

Increasing the maturity of a SOC allows analysts to stop fighting fires and focus on higher value work. With careful planning and the right combination of automation and standardized processes, a mature, effective, and world-class SOC can be established.

The danger of alert overload

The cybersecurity landscape has become increasingly hostile, and teams must deal with an ever-increasing barrage of security alerts. Teams have reported spending nearly a third of their time simply dealing with false positives, and we have long since passed the tipping point where these numbers can be dealt with on a manual basis.

Few firms can afford large teams, and even an army of analysts will not be able to comfortably tackle hundreds of alerts a day in addition to their other duties.

This is exacerbated by the fact that the on-going skills gap means recruiting and retaining a full team of analysts has become an increasingly costly proposition. Few firms can afford large teams, and even an army of analysts will not be able to comfortably tackle hundreds of alerts a day in addition to their other duties.

In addition to the sheer number of alerts they must deal with, SOC teams are hampered by inefficient processes. Many analysts end up using an ad-hoc suite of security solutions cobbled together from different providers and great deal of time can be wasted every day as analysts swap back and forth between different solutions.

There is no easy way to compare data from different tools to identify trends and more complex threats. Uniting solutions under a single

management system can help to win back lost time and establish a single view of threat data.

The impact of a burnt-out security team

The frustrations of burnt-out teams can build to the point where analysts will decide to quit their job in search of less stressful positions.

In the short term, this alert overload means an increased potential for high-risk threats being missed as analysts attempt to slog through as many alerts as possible alongside their other duties.

Aside from the immediate security issues, this kind of environment poses some serious long-term problems. The frustrations of burnt-out teams can build to the point where analysts will decide to quit their job in search of less stressful positions. We have found that around half of security personnel are considering changing roles at any given time. Not only will they be taking their experience and skills with them, but the ongoing cyber shortage means finding a replacement may be a long and costly process.

A team that spends most of its time trudging through alerts and running to put out security fires will also have very little time left for any higher-level strategic activity. This might include undertaking in-depth risk analysis and establishing improved security strategies and processes. Without this activity, the organization will struggle to keep up with evolving cyber threats.

How effective automation helps

Automation is the key to getting out of this rut. The more time consuming and low-value manual

Security teams need to be able to produce thorough documentation for all activities before they can begin automating them.

activities that can be automated, the more time analysts will have for more strategic activity. However, automation must be implemented correctly for it to have a real impact. The underlying processes and activities must be well understood and mapped out before they can be automated properly.

Security teams need to be able to produce thorough documentation for all activities before they can begin automating them. Implementation is a gradual process, starting with the most important tasks that will generate the most value and make the biggest contribution to protecting the organization from cyber threats.

Investigating and responding to alerts is a particularly strong area to focus automation efforts on, as it will greatly improve the efficiency of the SOC team, enhancing both their ability to detect and close threats, and the quality of their work environment.

The importance of playbooks

To effectively automate their alert responses, SOC teams will need to create playbooks of their processes, based on their knowledge and experience of different threats.

Processes can then be enhanced with automated tools, gradually reducing the level of manual work required and, in many cases, phasing it out altogether.

Many low-level security alerts such as malicious

emails can be investigated and closed without the need for any human intervention at all.

Taking things a step further, automated processes can be handled by a single focal point such as a Security Orchestration, Automation, and Response (SOAR) platform.

Playbooks will also help to increase a SOC's efficiency and maturity outside of aiding in automation. For example, if an analyst must pass on an issue to a colleague as their shift has ended, thorough documentation will make this a quick and easy task without the need for lengthy and redundant discussions.

Creating playbooks for each threat an organization might face will also improve the team's capabilities when a crisis occurs. Having a detailed set of processes will make it easier to tackle threats such as ransomware outbreaks or compromised user accounts and will also assist in automating as much of the process as possible.

Creating playbooks for each threat an organization might face will also improve the team's capabilities when a crisis occurs.

While SOC's will continue to have to deal with an ever-increasing volume of incoming threats and a shortage of experienced staff, improving their maturity and efficiency will help them keep up the pace without burning out their staff.

By developing detailed playbooks of scenarios and procedures, teams can implement more efficient, automated processes that will free staff from spending all their time sifting through alerts and enable them to better protect the organization.



Top tips for preventing SQL injection attacks

Brian Vermeer

Developer Advocate, Snyk

In the wake of the Colonial Pipeline attack and other high-profile cases, IT teams may be scrambling to shore up their endpoint protection. But those in the developer community know security weaknesses don't begin and end there; write code improperly or with insufficient security, and you're also coding in future web attacks.

Web vulnerabilities are an issue that affect even the biggest tech companies. They cover a host of different coding issues, but the examples above include a very specific type.

A zero-trust approach

SQL injection is one of the most dangerous and most common vulnerabilities, but fortunately there are several best practices developers can follow to

ensure there are minimal chinks in their armor.

The first is to ensure that client-side input validation isn't the only line of defense. This validation is a great tool for improved user experience, but it doesn't work as a security mechanism.

It's easy to remove client-side validation by altering JavaScript code loaded in the browser or do a basic HTTP call to the backend in a client-server architecture with a parameter that causes an SQL injection. Developers should be treating everything a client sends as potentially harmful and should therefore be validating on the server-side, ideally as close to the source as possible.

Developers should also think carefully about database user privileges. All SQL injection attacks are harmful, but some are more harmful than others: accessing user information is one thing but altering or deleting it is another.

Developers should be treating everything a client sends as potentially harmful.

To minimize the impact of an SQL injection, developers should be strategic about an application's privileges on a database. Does a specific application really need the ability to read, write and update all the databases? Is it necessary for it to be able to truncate or drop tables?

In addition to not allowing every application free reign over a database, it is also unwise to have a single database user for an application. Making multiple database users and connecting them to specific application roles works in the same way as fire doors work to contain a fire: it prevents an attacker from quickly taking over an entire database.

Parameters are the best defense

A critical way developers should protect themselves is by using prepared statements and query parameterization. A lot of languages come with built-in features that help prevent SQL injection, and so when writing SQL queries you can use a prepared statement to compile the query.

Many people believe that working with stored procedures is a good way to prevent SQL injection, but this is not always the case.

Prepared statements can be used to perform query parameterization, which limits the SQL statements that can be entered: a developer creates a base query with placeholders and then user-given parameters can be safely attached to these placeholders. When using a prepared statement and parameterized queries, the database will first build the query execution plan based on the query string with placeholders, and then send the (untrusted) parameters to the database.

As the query plan is already created, the parameters do not influence this anymore and this completely blocks injection. Prepared statements with query parameterization are therefore the best defense against SQL injection.

Parameterization is also paramount when working with stored procedures. Many people believe that working with stored procedures is a good way to prevent SQL injection, but this is not always the case. Just like any SQL queries created within an application, a stored procedure can be maliciously injected. Therefore, as with SQL queries, developers should parameterize the queries in their stored procedure, rather than concatenate the parameters, to protect against injection.

However, there are some situations where prepared statements are not available. If a certain language does not support prepared statements, or an older database doesn't allow developers to supply the user input as parameters, then input validation is an acceptable alternative.

Teams should ensure that input validation relies on allow-listing and not block-listing - using a well-maintained library or creating a rule that describes all allowed patterns with, for instance, a regular expression. Of course, even if prepared statements are available, input validation is a must.

Multi-layered security and stringent checking

In addition to parameterization and input validation, developers should consider using an object-relational mapping (ORM) layer to protect against injection. This transforms the data from a database into objects and vice-versa, reducing explicit SQL queries and therefore the risk of SQL injection attacks. However, it should be noted that vulnerabilities can still be created within ORM libraries if the wrong or outdated versions of Sequelize or Hibernate are used, so developers must be vigilant.

Ultimately, whatever security strategies are deployed, a strict reviewing system must be in place to review code and flag any vulnerabilities. Code review and pair programming do allow for this, but with manual reviewing processes there are always margins of error. For the highest levels of security, developers should look to specifically designed scanning tools to automatically check for SQL injection vulnerabilities and alert them to any weaknesses in their code.

SQL injection attacks are a dangerous online threat, but they can be defended against. With a zero-trust approach, the use of prepared

statements and parameters, and a stringent code-checking process, developers can block any injection attempts. As cybercrime grows in tandem with digitalization, it's more important than ever that developers write security into the heart of their code.

Ultimately, whatever security strategies are deployed, a strict reviewing system must be in place to review code and flag any vulnerabilities.

The image shows a promotional graphic for a Help Net Security report. At the top, the Help Net Security logo is displayed. Below it is a tilted image of the report cover, which features the title 'XDR REPORT' in large white letters, the subtitle 'Q4 2021' in smaller white letters, and a 3D geometric graphic. At the bottom of the graphic, the text 'Help Net Security' is visible. Below the report cover, the text 'Help Net Security report: XDR' is written in yellow. At the very bottom, a yellow button with the text 'FREE DOWNLOAD' in black is shown.

Help Net Security

XDR REPORT

Q4 2021

Help Net Security report: XDR

FREE DOWNLOAD

THE (ISC)² CERTIFICATION PREP KIT

— Your Ultimate Guide to Exam Planning —



We know that preparing for the CISSP, CCSP, or another (ISC)² certification exam is a big commitment and it can be difficult to know where to start. Find all the tools you'll need to conquer your exam in the (ISC)²'s Certification Prep Kit. From free study tools to courseware previews, we've put together a guide of industry-leading resources that will help you plan your path to certification success.

Your free (ISC)² Certification Prep Kit includes:

- Fast facts on (ISC)² training
- 3 training myths debunked
- Official course previews
- Justification letter for certification
- Choosing the right study tools
- 7 tips for certification success

Kickstart your journey to certification and join over 160,000 talented cybersecurity professionals who are (ISC)² certified. Take the next step today!

Get My Free Kit

