CYBER PROTECTION
MAGAZINE
2 || 2025

Insurance & Encryption

US
the new
'Axis of Evil'?

Cyber protection
for the 90%

quantum encryption ++ understanding cyber insurance

CONTENT

2.25

Editorial

Welcome to the spring 2025 edition of Cyber Protection Magazine. In our last issue, we predicted that 2025 will be a very interesting year. Well, looking at what happend in the past two months, we apparently were right. Unfortunately. However, while there are some article pertaining to what happend in the world (p. 11, 14) we actually wanted to focus on insurance and encryption. So we asked some of our contributers to write up some articles – here's the result.

We're starting off, however, with a dream we've had ever since starting Cyber Protection Magazine Our initial goal was always make cybersecurity accessible and actionable for organizations of every size. Our new partner, Lupasafe, provides a service to our primary audience, the small-to-medium enterprises that generally get ignored by most cybersecurity companies. We are not only helping to promote Lupasafe, we have tested it, use it, and endorse it. Read about their solution in our cover article.

Next, Holly Burton breaks down the ever-evolving landscape of cyber insurance, helping you decide whether first- or third-party coverage is right for your organization, and explaining how Tech E&O policies are filling critical gaps. If you've been on the fence about premiums versus peace of mind, you won't want to miss it.

Quantum computing is no longer tomorrow's problem. David Close and Christina Cravens each outline the race toward post-quantum cryptography—where NIST standards, "harvest now, decrypt later" threats and crypto-agility converge. Their clear-sighted roadmaps will help you future-proof your key management and encryption strategy today.

In "Finding the Silver Lining in the Signal Chat Leak", Brian Hill turns a high-profile blunder into a case study in personal-device hygiene, data-broker removal and the rise of enterprise-grade protection for executives and their families. It's a reminder that the weakest link is often where we least expect it.

Dwayne McDaniel and our "Scam Bucket" series both delve into the human element—whether it's non-human identities leaking secrets in your CI/CD pipeline, or would-be helpers hijacking your home printer. Their practical advice underscores a simple truth: technology alone can't solve a problem built on human behavior.

Then, at the heart of this issue, Lou Covey returns with a pointed commentary on geopolitics and cybersecurity, juxtaposing national agendas with our industry's ethical imperatives. And for those curious about "Encryption in Use," be sure to read our primer (p. 19) on why data-at-rest and fully homomorphic approaches deserve your immediate attention.

Rounding out the magazine, you'll find deep dives into privacy versus national security , the tools and mindsets that underpin modern security hygiene (p. 23), and AI's growing role in building tomorrow's security analysts, Finally, we close with "What CIOs Should Prioritize", a concise blueprint for leaders balancing innovation, risk and budget in 2025.

Whether you're an executive, an engineer or somewhere in between, we trust these articles will spark new ideas and guide your next steps. Thank you for joining us on this journey—here's to a safer, smarter year ahead.

Cyber protection for the 90%

AUTHOR: PATRICK BOCH

The introduction of a Cornell University study said, “Small and Medium Enterprises (SMEs) are pivotal in the global economy, accounting for over 90% of businesses and 60% of employment worldwide. Despite their significance, SMEs have disregarded from cybersecurity initiatives“

This is not just a reality for SMEs it is also true when you look at what cybersecurity companies provide. Most focus on medium to large customers, solving problems only corporations with complex IT landscapes have. And if that isn’t the focus they solve largely non-existant or hypothetical problems (but that is another story for another day).

The study went on to say. “The existing research indicates that the main challenges to attaining cybersecurity resilience of SMEs are a lack of awareness of the cybersecurity risks, limited cybersecurity literacy and constrained financial resources.”

That second point — security awareness — is a founding issue for Cyber Protection Magazine. And ever since we started, we were looking for a partner who could take care of the rest: providing a toolset for those cybersecurity risks that really matter and raising awareness through training.

Finally, we have found that partner: Lupasafe. Their target customers are either SMEs directly – or MSP (who usually serve SMEs). Lupasafe essentially brings two things to the table: A tool which gives an overview of the security status for the most important

topics. And a cybersecurity training module, including phishing tests. If you know how Cyber Protection Magazine works, you will know that we're not falling for marketing speech. In this case we've actually tried and tested (and will keep) the Lupasafe solution for ourselves, as it gives us just the amount of insight we need, not trying to scare us with hypothetical risks which we actually don't have.

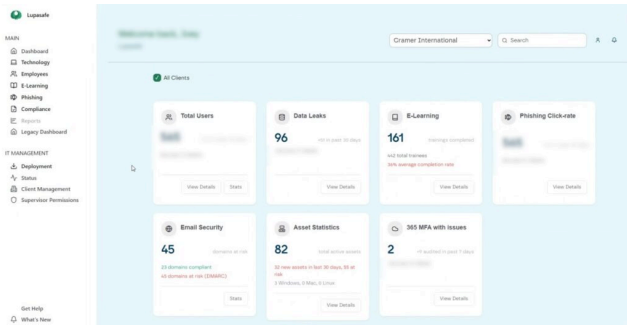
Here's our honest review about Lupasafe and what it does for us.

> "it gives us just the amount of insight we need"

A little background: The team behind Cyber Protection Magazine is small, but nevertheless scattered across the globe. It's also not one company, but a joint venture of two companies. Which means we have different e-mail addresses, different websites (besides our main website at cyberprotection-magazine.com), quite a few cloud services for collaborating and file storage. So far, so common for SMEs. The one thing we don't have is our own internal network, but then our two companies do have their own networks, too.

How does Lupasafe secure us then? The first thing we did is we entered those assets we have – our websites, domains and e-mail addresses. And within a few minutes we've had the first report on potential risks of these assets, shown in a dashboard-like overview.

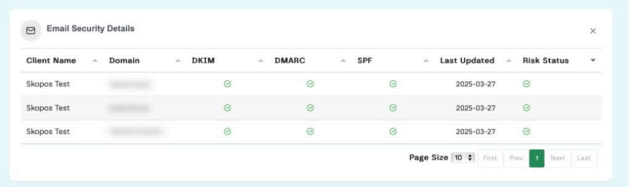
For the domains and websites, Lupasafe shows all relevant information, which are:



The Lupasafe Dashboard

- Open ports
- Security headers
- DKIM/DMARC/SPF Scan
- SSL/TLS Scan
- Vulnerabilities
- Dmarc reports

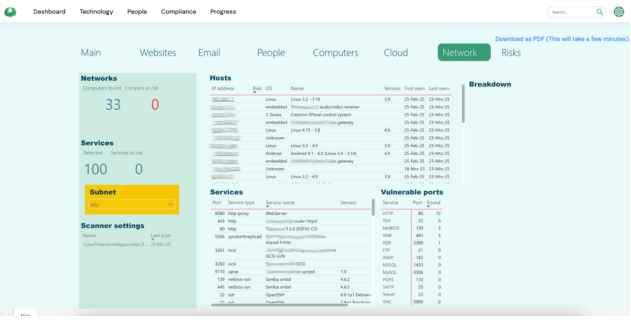
If you don't know what all of these mean – don't worry, your admin should know. And if they don't, Lupasafe has a really helpful documentation. At least myself, as a half-nerd, was able to quickly grasp what's behind those terms I didn't know previously. Also, that list pretty much represents the most common risks on domain and website level you can have.



DMARK? DKIM? Lupasafe has a helpful documentation to guide you through these terms

For each topic, you can then drill further down and see the risk level (high, medium or low), a more detailed list and explanation where applicable.

Similarly, Lupasafe will look at cloud instances. Currently, they support Microsoft Office 365 and Microsoft Entra ID – since at CPM we have neither, we couldn't verify how these assets are handled. What we could do was scanning our internal network. That was a little tricky, since our network(s) are so small that we don't have a real server – the networkscanner Lupasafe is providing, though, can only run on Linux and Windows machines. Luckily, there is a virtual Windows machine which is hardly ever needed which we could use for this purpose. Hence, we installed the network scanner and after a bit of crawling through our network, it also presented us the results. "Unfortunately", the risk within our small network seems to be comparatively small: none of the devices in the network returned a risk.

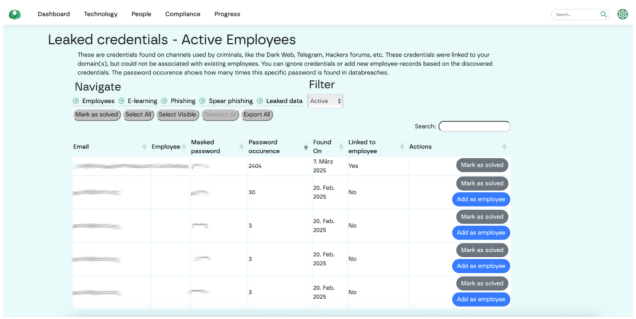


Results of a network scan

Domains, Cloud services and the network scanner covered the technology side of things – more interesting is the what Lupasafe refers to as "people". This section covers two topics: Leaked data and the actual Lupasafe cybersecurity training.

> "all information you need"

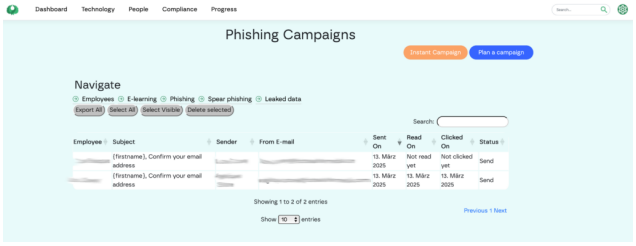
The leaked data sections shows – based on the e-mail addresses of your employees – whether those were “pawned” in any known data leaks which occurred in the past few years. It even shows you the first and last letter of your password, so that each employee can verify if that password might still be in use, and, if that leak was actually linked to an employee. It also gives you the name of the breach and the year of occurrence. Again – pretty much all information you need in this context. However, those more technology related topics, which essentially require scanning the web and the different company assets, are reactive, not proactive.



Was my data leaked? Lupasafe will tell you

Enter the main part of the “people” section: phishing – divided into regular phishing and spear fishing, and the e-learning program. Phishing is one of the most commonly used techniques for cyber criminals to retrieve credentials. Usually, they will send an e-mail which sounds like it’s an official e-mail from your bank, insurance company or other provider, asking you to click a link. The clicked website looks almost identical to the actual website of the provider, so you might be inclined to enter your credentials there. In the past, both the phishing e-mail and the fake website were often easy to identify. These days, with AI and other tools, they are almost not distinguishable from their real counterparts.

The phishing module in Lupasafe will send a fake e-mail to your employees to see whether they’ll fall for that technique. Lupasafe also offers spear phishing – same thing as phishing, just personalized. If your employees fall for the phishing, they will be directed to the e-learning module. As an administrator, you can plan phishing campaigns for your company or start an “instant” campaign – after running this, you will also see the results of these campaigns.



The phishing module of Lupasafe

Last, but not least, is the e-learning module of Lupasafe. This, however, as well as our conclusion for their solution will be covered in the second part of this article.

Since the Lupasafe solution covers all of our needs and we can imagine that it will also cover the needs for most SMEs, we partnered with Lupasafe, providing you, our readers, with the possibility to secure their assets and people just like we are doing. If you want to sign up for Lupasafe, sign up here:

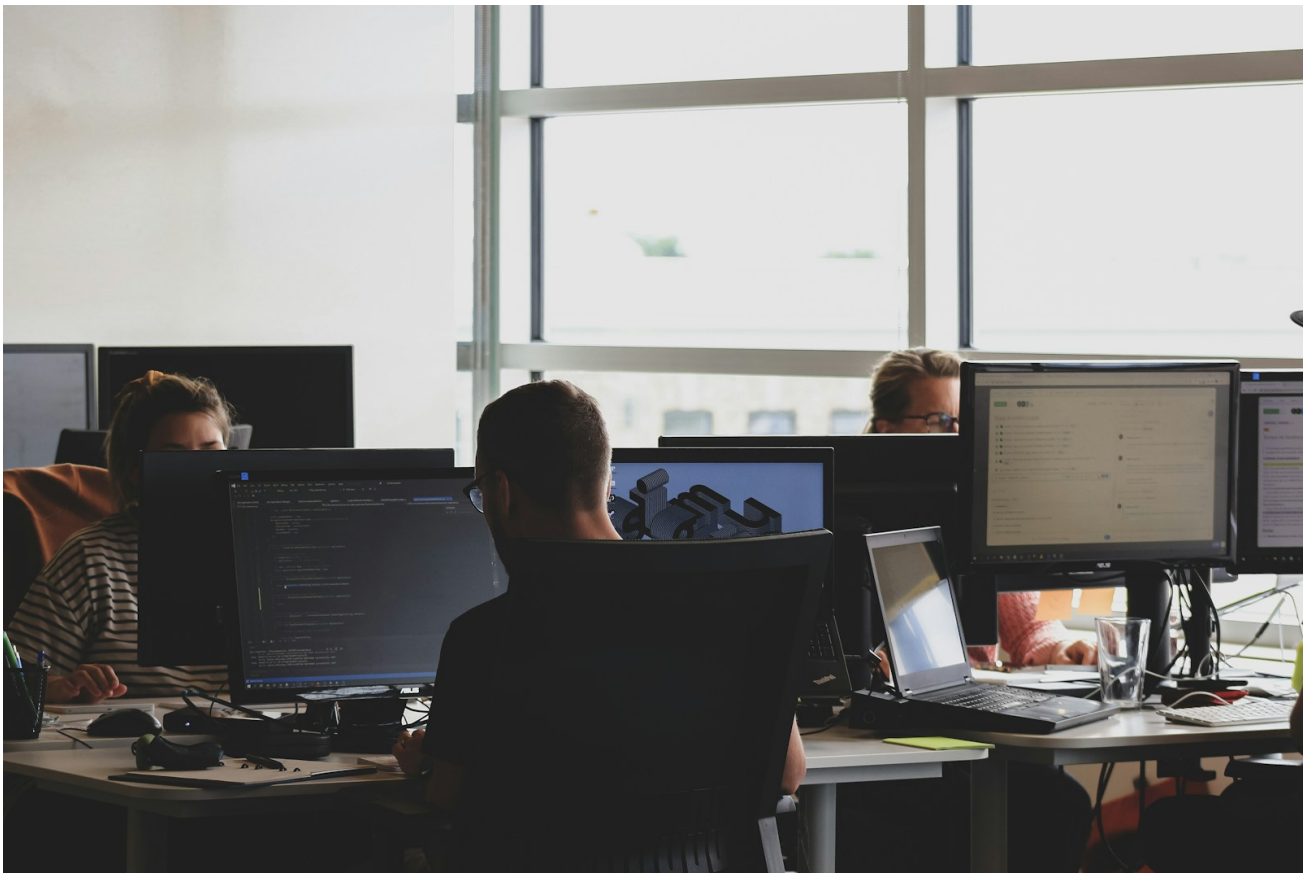
For more information on Lupasafe visit https://lupasafe.com/

PATRICK BOCH

Co-Founder and Editor for Cyber Protection Magazine

Cybersecurity Hygiene Starts with People – and the Tools That Support Them

AUTHOR: RICH KANADJIAN



Companies dedicate plenty of money to cybersecurity tools like firewalls and threat detection systems. While these are valuable investments, surprisingly often, breaches happen because of simple human mistakes – clicking an unknowingly malicious link in a hurry, reusing an old password, or losing a USB drive. The truth is that people are the most important actors in cybersecurity, although they are frequently overlooked. IT leaders who understand this can build a workplace culture where good digital habits become second nature, aided by technology that makes it easier to stay safe.

CYBERSECURITY HYGIENE: EVERYDAY SECURITY BASICS

Like personal hygiene, cybersecurity hygiene is about establishing healthy habits so that the small, consistent things employees do every day properly protect sensitive information. This includes checking who an email is *really* from before clicking on links

or attachments, locking your computer when you step away, not plugging in unfamiliar USB drives, and using different, strong passwords for each account.

The problem is, the typical annual cybersecurity training session with long presentations is quickly forgotten by most employees, if they were paying attention in the first place. A better approach is to weave in regular, short, interactive reminders into the regular run of business. Things like quick phishing tests or weekly security tips work well because they focus not just on *how* to do something (like spot a fake email) but *why* it's important.

SECURITY STARTS AT THE TOP

Building a security-conscious culture really starts with leadership. When managers and executives consistently use things like multi-factor authentication and share files securely, it sets the standard. Employees see it and are more likely to follow their lead. Plus, giving a shout-out to teams that do well on security exercises helps turn cyber hygiene from just another rule into something the whole team can be proud of.

WHY PASSPHRASES BEAT COMPLEX PASSWORDS

The standard "complex passwords" full of symbols and random numbers might seem secure, but they often cause employees to resort to poor cyber hygiene in order to remember them, like writing passwords on sticky notes, using variations of the same password everywhere, or making tiny changes when forced to update.

Instead, experts like those at NIST now recommend using **passphrases**. These are long strings of simple words, like "Blue-guitar-autumn-lantern." They are much easier for people to remember but significantly harder for automated hacking tools to crack. When you pair passphrases with multi-factor authentication and straightforward ways to recover accounts, people get less frustrated and are more likely to stick to the security policies.

PROTECTING DATA ON THE GO WITH HARDWARE ENCRYPTION

Even the most careful employee can lose a laptop or have a USB drive stolen. That's where hardware-encrypted storage becomes essential as a last line of defense when other hygienic practices fall short. Drives with encryption built right in automatically protect the data, stopping anyone without the right credentials from accessing it even if they have the device. Unlike software encryption, which relies only on software, hardware encryption is physically part of the drive and is not vulnerable to the same kinds of software attacks or brute-force password guessing.

When choosing encrypted drives, look for ones certified by trusted groups (like FIPS 197 or FIPS 140-3 Level 3). This certification means they meet high encryption security standards. Also, drives with digitally signed firmware are important because they help protect against nasty threats like "BadUSB," where malware tries to sneak in through a compromised USB device's firmware.

AN RSA-WEEK CHECKLIST FOR BETTER CYBER HYGIENE

- **Know Your Sensitive Data:** Figure out what information needs the most protection and keep track of where it goes.
- **Back Up Regularly:** Make sure you have reliable, air-gapped backups of critical data. This is your safety net against ransomware and other data loss.
- **Keep Training Short and Sweet:** Use frequent, bite-sized security reminders and activities to keep awareness high without causing fatigue.
- **Use Hardware-Encrypted Storage:** Provide employees with secure, hardware-encrypted USB or external SSD drives for any data that needs to leave the network, and set up endpoint protections to block unknown devices by default.

While advanced cybersecurity technology is definitely still useful to help close security gaps, it can't fully cover the risks that come from everyday human habits. Organizations that put real effort into the human side of security build a much stronger first line of defense. By making security guidance clear, reinforcing it regularly, and providing technology that supports good habits, companies can significantly lower their risk. Ultimately, a workforce that practices good cybersecurity hygiene is a very tough barrier for attackers to overcome.

RICH KANADJIAN

Global Business Manager, Encrypted Unit at Kingston Technology

Scam bucket: Tech support fraud

AUTHOR: LOU COVEY

Before you call tech support, be wary of who you call

Dealing with wonky printers is a universal frustration. According to Gartner studies, printers are by far the biggest technology problem, racking up 50 percent of all technical support calls worldwide. And that makes them a very profitable scam.

Here's how it works. You're sitting at home and want to print out a bill, letter, or other document and the printer hangs up. The little wheel is just spinning and spinning. After multiple tries you decide to call tech support to fix the problem. After 2 hours of sitting listening to the same song, interrupted by the recorded voice telling you your "call is important," you start surfing for some sort of help. Your results show three or four sites for printer support and a free chat service.

You click one of them, still waiting on your phone for help, and immediately get someone in the chatbot who is very helpful and asks if they can be connected to your computer to see what the problem is. In the hope of being freed from frustration you click on a link and suddenly your "savior" is moving around your computer downloading "the latest printer driver." It is only much later that you find he has found your banking information and has sucked your account dry.

BILLIONS IN LOSSES

You are not the only one that gets caught. In 2025, the FBI's Internet Crime Complaint Center received over 17,000 complaints about tech support scams, resulting in over $3.4 billion in losses. If Gartner's numbers are correct, that means about $1.7 billion in those losses are from people just trying to print out a picture or document.

Some of that money goes to search companies like (looks at notes) Google. Since they are immune to lawsuits (thanks to the FCC's section 230) for giving these scammers first priority on search results, they get to make money from these organizations who pay for that placement. Of course as soon as the scammers are identified they are taken down. Then they reorganize under a new identity and do it again.

The companies that make these printers have some culpability. Maybe a lot. HP, for example, recently launched, and then took down a system that intentionally made people wait longer for tech support.

When you called HP support for anything, a recorded voice, citing high call volume, gave you a choice. Either go online to HP support and find a fix there, or wait on the phone 15 minutes before you were placed in a queue to wait even more time to talk to an agent. However, when they found out they could be sued for that they quickly removed the 15-minute wait.

UNDERFUNDED INTENTIONALLY

Beyond that, technical support is notoriously underfunded by corporations, which is one of there reasons they outsource it to third-party companies in Southeast Asia. But they also make the process intentionally frustrating to make customers go away, because that saves them money as well.

Printers are incredibly complex devices combining software, hardware and mechanical systems that have to be constantly maintained and updated. But they are also incredibly cheap because the printer companies make money selling ink. They would rather you just buy a new printer than fix it.

But there are things you can do to avoid getting scammed and still have a working printer.

- Update, update, update: Printer drivers don't get updated that often. When they do it is extremely important to install them, more so if they are security updates. Ignoring the updates can effectively brick the printer and you will have to buy a new one.
- Check before you click: If you do the updates and still have a problem that needs support, make sure it is legitimate. One way is the way you phrase the search term. For example, when we asked for "HP printer support" we got links to HP. Asking for "HP printer help" got us a list of known scam sites.
- Zero Trust: Ignore anyone contacting you claiming there is a problem with your system. Go to the company website before you allow them access.

LOU COVEY

Lou is Chief Editor of Cyber Protection Magazine

STABILITY MATTERS IN CYBER RISK INSURANCE

Providing reliability against unpredictable and evolving cyber threats.

The right cyber risk insurance partner can protect against global privacy and network security risks.

With over 80 years in business and an A.M. Best rating of A++ XV, the highest rating a carrier can achieve, Safety National has the longevity and stability to ensure we'll be there when you need us.

Trusted
SAFETY NATIONAL
Since 1942

Safety National provides uniquely tailored solutions, including:

- Standalone and blended cyber risk offerings
- Reliable excess capacity
- Specialty claims and underwriting expertise

LEARN MORE
about our cyber insurance offerings at SafetyNational.com.

TOKIO MARINE
GROUP

User Privacy vs National Security

AUTHOR: TIM ERLIN

The idea of encryption backdoors for law enforcement or government is not new. Governments around the world have been advocating for and even passing wiretapping laws since the 1990s. Recently, this extended to Apple, with the United Kingdom demanding that Apple allow the government access to people's personal data under the Investigatory Powers Act. Issued in January but still undisclosed, the order targeted Apple's Advanced Data Protection (ADP) feature. While this is not the first time that encryption backdoors have been a central talking point around government surveillance, this particular outcome opens the door to a global discussion as to government reach and individual privacy.

For now, in response to the UK's filing, Apple disabled ADP for users in the UK, stating: "We are deeply disappointed that our customers in the UK will no longer have the option to enable Advanced Data Protection (ADP), especially given the continuing rise of data breaches and other threats to customer privacy. Apple remains committed to offering our users the highest level of security for their personal data and we are hopeful that we will be able to do so in the future in the United Kingdom."

Backdoor Encryption: security trade-off

The dueling arguments for backdoor encryption are that access to communications is critical for national security or investigating crimes, it violates privacy principles, and criminals can exploit any backdoor. The reality is that requiring encryption backdoors is a shortsighted solution to a real-world problem. Hackers can exploit all kinds of products that don't have intentional backdoors. Knowing this, any intentional backdoor access can be used for malicious purposes. Further exacerbating the situation, criminals are using encrypted communications to conduct their activities. In the end, it's not possible to create an encryption backdoor that isn't accessible to criminals. More importantly, there's no guarantee that the government or law enforcement won't act criminally either.

While Apple intentionally built a reputation for privacy, they cannot ignore the UK government's demands. Ultimately, Apple decided to end the ADP feature for UK customers – a power move by Apple.

What does this mean for consumers?

For UK users, these changes mean that the categories of iCloud data covered by the ADP will no longer be end-to-end encrypted. That includes iCloud backups, photos, notes, and more. Apple employees and law enforcement will now have access to those data categories. Standard data protection will still apply, encrypting other specific categories of data, such as passwords and health information. For the average user, the breakdown of categories and encryption can be complex to understand. Outside the UK, for now, there's no change.

An ideological bifurcation exists between people who believe in privacy as an absolute right and those who see it as fundamentally limited. Regardless of one's ideological position, no evidence supports a technological solution to safely backdoor encryption. History has shown that process-based solutions, such as requiring oversight and judicial review, will likely be abused. And while this fight is playing out in the UK only, it's likely to surface elsewhere in the future. Given that the current U.S. administration seems to lean towards privacy being a limited right, it's likely that the idea of encryption backdoors will resurface here in the near future.

TIM ERLIN

Security Strategist at Wallarm

Finding the Silver Lining in the Signal Chat Leak

AUTHOR: BRIAN HILL

All it took was a lapse in judgment and a user error to pose a national security risk and ignite a major public firestorm. The recent Signal chat leak—where a government official accidentally added a journalist to a highly sensitive group chat using a consumer-grade app—offers us a chance to learn from mistakes like this and better protect ourselves.

Whether you're a politician, a corporate leader or even a philanthropist, you can never lose sight of the fact that there is no true safe haven. It doesn't matter if you're in the office or at home, you are always in the line of fire from a cyberattack and so is your family. While high-profile individuals and their families often don't see themselves as targets when they're at home or traveling, the harsh truth is that they are, and it's only getting worse.

According to the 2025 Ponemon Institute research study, *Deepfake Deception: How AI Harms the Fortunes and Reputation of Executives and Corporations*, 51% of CISOs reported being aware of cyberattacks targeting the personal accounts of their executives or their family members—up from 42% in 2023.

THE NEED FOR HOLISTIC SECURITY

We live in an interconnected world that demands a holistic approach to security—one that safeguards not only our professional and personal lives, but also, by extension, the well-being of our families. Nation-states and cybercriminals will always choose the path of least resistance—and personal devices, email

accounts, and other online platforms often present the easiest points of entry. Digital attacks on key individuals at home—through their personal devices or even through loved ones—have become a growing tactic among both cybercriminals and nation-state actors.

By adopting a holistic approach to security, you can reduce digital and physical risks for yourself and your family in their personal lives, on personal devices, and on home networks. This affords you peace of mind, knowing that you and your family are protected, with all potential threats carefully monitored and neutralized by a dedicated security team—24/7/365.

REMOVING PERSONAL INFORMATION FROM DATA BROKER SITES

Personal data is widely accessible through open-source intelligence, making it easy for cyber criminals to find information associated with an individual. Much of this information—personal phone numbers, personal email addresses, and physical addresses—can be found on data broker websites or on the dark web—places where cybercriminals and nation-state actors routinely buy, sell, and trade sensitive data.

Once a cybercriminal obtains this information, they may launch a smishing attack by sending a fraudulent text message or a phishing email to a known email address. If the target opens the message on their phone—whether through the email app or directly via the text—it can trigger malware that compromises the entire device, granting the attacker full access.

Data removal services will help reduce your digital footprint and minimize this risk. Through modern Digital Executive Protection (DEP) capabilities, security teams will work for you to continuously search and eliminate personal information from data broker sites and the dark web, making it harder to find and making you less vulnerable to a cyberattack.

USING ENTERPRISE-GRADE TECHNOLOGY TO STAY AHEAD OF CYBER CRIMINALS

Recognizing your security limitations is also crucial. For example, sharing sensitive or classified information on consumer-grade apps like Signal can be a recipe for disaster. The same can be said about communicating over poorly secured public Wi-Fi instead of an encrypted virtual private network (VPN). Bad actors are always snooping, looking for gaps in security and vulnerabilities to exploit.

While there's no fail-safe against the careless mishandling of classified or sensitive information, strengthening security with advanced technology can help reduce the risk of exposure. For example, proactively monitoring and securing cell phones, tablets, and computers with the same enterprise-grade tools that are used to secure corporate networks and devices will provide an extra layer of protection.

BRIAN HILL

Head of Security Services at BlackCloak

Commentary: Is the US the new 'Axis of Evil'?

AUTHOR: LOU COVEY

Ordering investigations and revoking security clearances for former CISA director Chris Krebs, along with several other employees of federal contractor SentinelOne is but the latest step downward for US credibility. President Donald Trump bears the entire responsibility for the decline into membership in a new "axis of evil." It may be time for the cybersecurity industry to recognize that the US government is not a customer it wants for the next two to four years.

President George W. Bush coined that term in 2002 that included certain countries, including Iran and North Korea, as the "Axis of Evil" in the world for their support of terrorism. The current administration's ignorance of security in "Signalgate", the decimation the US intelligence infrastructure, and a growing trade war, all give credence to US the image of a new source of international danger in both incompetence and intent. Cyber Protection Magazine is not the only publication to point this out.

FEW WILL SPEAK OUT

This latest attack on free speech and truth in the

Krebs memorandum was met with almost total silence from the US cybersecurity industry. Several prominent voices responded to our requests for comment. All requested anonymity because their livelihood depend on the "good graces" of Donald Trump.

One of the few brave souls willing to speak was Matt Blaze, McDevitt Professor of Computer Science and Law at Georgetown University. On a Mastodon post last week he said, "Trump's official denouncement of former CISA director Chris Krebs is chilling in substance and utterly Stalinesque in tone. By threatening anyone who hires him, it aims to render Krebs effectively unemployable."

Even SentinelOne's official statement was a bloodless capitulation to the order, rather than a defense of its employees.

Outside of the US, there is greater freedom to comment, a statement we never thought we would say in our lifetime.

"The old relationship we had with the United States, based on deepening integration of our economies and tight security and military co-operations, is over," said Mark Carney, Prime Minister of Canada. "The time will come for a broad renegotiation of our security and trade relationship."

Writing about the reversal of support for Ukraine, Janet Daley an American-born conservative journalist writing for The Telegraph in the UK asked, "If the American president is deliberately choosing to damage the security of a nation, which we unambiguously regard as friendly to defend itself against an invading enemy, can we trust the US government with the security information which we would once have expected to share in our mutual interest?"

DISGRACEFUL AND DANGEROUS

"The EO targeting Krebs and SentinelOne is disgraceful and dangerous," James Bore, a UK cybersecurity consultant and speaker, wrote to us. "Politicizing national security tools, and persecuting cybersecurity professionals actively fighting known disinformation, is a direct attack on our field. It places the infrastructure of the US at greater risk purely to satisfy a personal vendetta. This precedent is chilling for all who work in security, knowing their work is at the mercy of this level of petty vengeance."

In a recent podcast, Bore agreed with some pundits that Krebs and the other SentinelOne employees being targeted are in danger of incarceration without trial, especially in light of President Trump's interest in sending dissidents to an El Salvador prison. "If I were them, I'd be making flight reservations now."

That leads to asking, for at least the next two years, if it makes sense for the cybersecurity industry to do business with the federal government.

The experts providing anonymous insight rejected the idea that cybersecurity companies should or will step away from those contracts. One of the few that did comment publicly was Ian Thornton-Trump, CISO of MSSP Inversion6.

GREED 'TRUMPS' ACCOUNTABILITY

"Tech drives the US Government and will continue to be one of the largest customers," he said. "Corporate greed seems to win over altruism nearly every single time." But Thornton-Trump disagreed that this changes US security posture.

"US security remains in great shape. What has been removed is any sense of accountability for a security failure or violation. CISA never had enforcement powers, so the dismantling or reduction in capabilities will have a minimal impact on the overall cybersecurity posture of the USA, mostly because government-funded programs compete with commercial offerings."

However, Thornton-Trump calls the memorandum "pure mob boss" mentality. "Chris got political by accident or design and has now paid the iron price."

Outside naked greed, does it make sense to support the Trump administration? The US is not just the federal government. There are state, county and municipal governments needing security services. Adjusting marketing targets for that business could more than make up the loss of revenue from the federal revenue.

Like much of the world is discovering, there is business outside of Washington, D.C. It might be time to hedge the bets.

LOU COVEY

Lou is Chief Editor of Cyber Protection Magazine

Understanding Cyber Insurance

AUTHOR: HOLLY BURTON

Cyberattacks continue to be among the top business risks. A recent Hiscox survey showed that cyberattacks increased in 2024, with 7 in 10 (69%) U.S. companies reporting an increase in cyber-attacks compared to the previous year. And while large companies face higher risks, companies with 50-249 employees still saw at least 53 incidents on average. Also of note is that many companies are acknowledging that they are ill-prepared for attacks.

The fallout from cyberattacks range from financial to reputational. Through the lens of preparation, understanding your company's cyber insurance (or cybersecurity insurance) policy is critical. Cyber insurance is what protects you and your small business from the costs associated with data breaches and/or other software attacks, including expenses for customer management, credit monitoring, legal fees and more.

Now more than ever, cyber insurance should be considered a must-buy for any business that uses a computer in their operations. This is especially true if your business is processing transactions via credit card or bank transfer, handling sensitive data (social security numbers, driver's license numbers, etc.) as well as traditional name, address or phone information. It is important to note that there are two prevalent types of cyber insurance – first-party and third-party coverage. The common use case is first-party, where a business would need to insure against its own cyber risks. Businesses that are responsible for their clients' cybersecurity would need third-party insurance.

One of the more common incidents that first-party cyber liability insurance can cover is when a data breach happens. In fact, most states now require a response when a business is impacted by a data breach (which is why it's important to frequently review your current policies). Unfortunately, ransomware attacks are also on the rise. If a bad actor steals sensitive information about you, your company, employers and/or customers, or if they lock you out of your system, cyber liability insurance can help with payments to meet these demands.

While less common for those in the IT, cybersecurity and/or other related technology industries, third-party insurance is also essential, especially if you are in a position to make software solutions on behalf of clients and/or directly manage their networks. Third-party insurance can help cover legal costs, settlement costs and/or court-ordered judgments.

Costs for cyber liability insurance may vary. Everything from the amount and what type of sensitive data that is handled, to the industry itself, will be factors in determining costs. It's also important to note that there are also exclusions from cyber liability insurance and those may include data loss or breach as a result of a mistake, natural disaster and/or a natural occurrence (i.e., power surge, fire, etc.).

To further protect technology companies, there is also technology errors and omissions insurance (or tech E&O), which bundles errors and omissions insurance together with cyber liability insurance. This bundling ensures maximum protection for IT companies that are on the front line of constant cybersecurity threats.

As the impact of AI or IoT grows, businesses may even need more protection. The same is true with frequent regulatory changes based on where your business is located, and/or the locations of the customers you serve. In the end, there is no better time than now to add a policy or review your existing one. Cybersecurity issues are not going away anytime soon, and cyber liability insurance provides peace of mind so smart businesses can focus their time and energy on what they do best.

HOLLY BURTON

Assistant Sales Director at Insureon

An encryption primer: Don't wait

AUTHOR: LOU COVEY

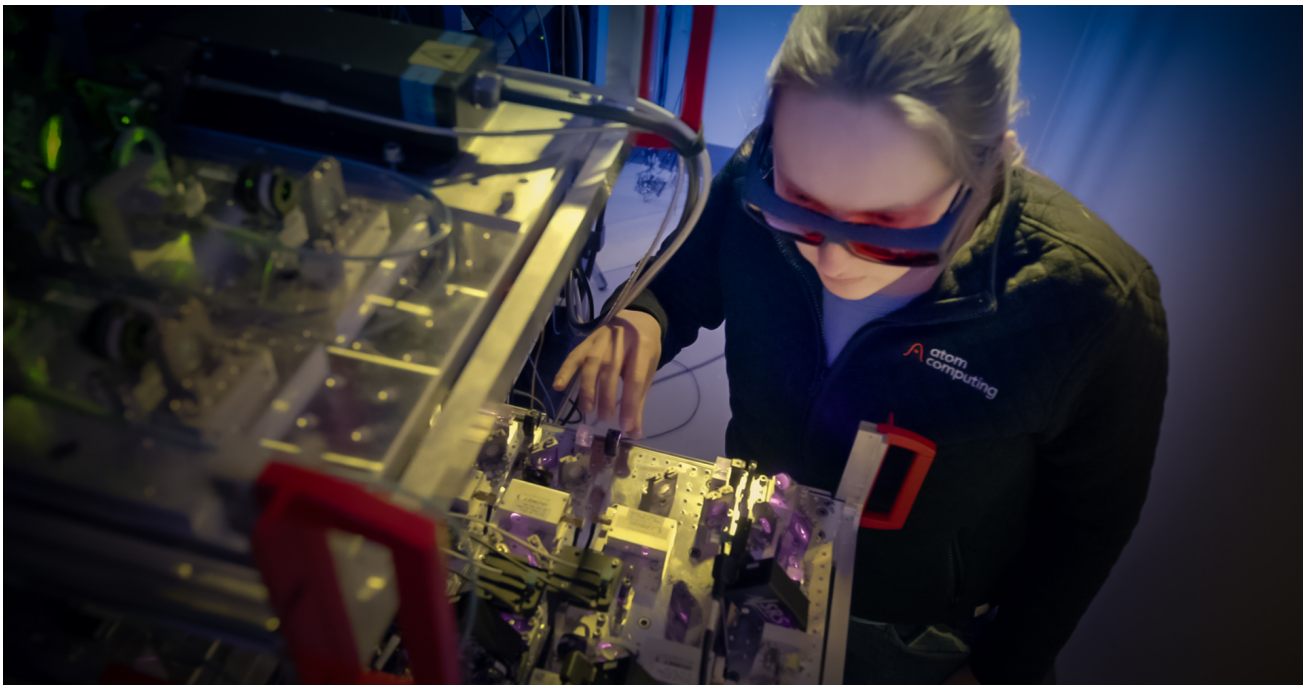


Photo by Atom Computing

Encryption became a hot topic in the news in the past month. The United Kingdom, Sweden, France and the EU are considering requiring "back doors" to encryption protections. The "Signalgate" scandal in Washington, DC started most people asking, "What is this encryption stuff?" So we decided to provide a primer on the state of encryption today.

While the technology behind encryption is complex, it is not new. The basic algorithms have been with us for decades, silently running on devices and servers, invisible to the user. The purpose is basic: to keep data safe from prying eyes, like criminals and nation states.

Encryption is also a good way of saving money and not just in avoiding ransoms. Insurance companies often offer up to 15% premium discounts to businesses demonstrating strong security practices, including proper data encryption. Encryption significantly reduces the risk of data breaches and their associated costs.

THREE STAGES OF ENCRYPTION

The process of encryption has three stages. First is data in motion. That's when you send or receive data. Second is data at rest, which is when you store data. Third is data in use, when you are creating new data, like when this article is being written. That last part is problematic and has yet to be incorporated widely, but more on that later.

The first process, in motion, is pretty well resolved. According to Google, 95 percent of all data in motion is encrypted. That means pretty much everything you send or receive has been made safe. That's the White House argument regarding the use of Signal to discuss the attack on Houthi camps in Yemen. "It's an encrypted messaging app!" Well, yes, the data you send is encrypted, until it lands on your digital device. Then it is unencrypted and stored for you to read it. That's the second process, data at rest, and it is not that secure.

THE PROBLEM OF DATA AT REST

In 2023, Thales said only 45 percent of data at rest is encrypted. Encryption, as a technology, has been perfected and in use for decades. One might wonder why everything in every major server isn't encrypted. The problem is that regulations requiring encryption of data are not too clear.

In regards to personal heal data, the HIPAA the regulation is generally interpreted that data at rest should be encrypted, but it does not explicitly mandate it. And that is also true for a lot of security regulations, including the EU's GDPR and California's CCPA/CPRA. Financial systems regulations do spell it out, like the Payment Card Industry, as well as US federal systems and education. But that leaves a lot of data unprotected and gives companies an out when things go bad.

SEE NO EVIL

Oracle is a big company that tends to acquire other companies, especially those who were Oracle customers. Some of those acquired companies, apparently, don't encrypt their data at rest and in March 2025, a breach was reported on Oracle servers, including Oracle Health. The data was stored on older acquired servers that were being migrated to more secure servers in the Oracle system. But not in time.

At first Oracle claimed they knew nothing of a breach, basically because they used a "see no evil" approach to data security, according to Ian Thornton Trump, CISO for managed security service provider Inversion6.

"It's a new and innovative legal defense to suggest If we don't believe we have had a security incident, then we don't really need to report it, right? Good luck with that defense when the inevitable class action occurs," he said. After Thornton-Trump talked with Cyber Protection Magazine, Oracle did admit the breach had happened, but for the purpose of defending against the class-action suit that was filed, again claimed it was not to their newer servers. Oracle, however, is not the only company with its head in the sand.

A LONG ROAD TO FULL ENCRYPTION

In the past two years, 90 percent of all stored data was created, according to Alexandra Borgeaud, an analyst for Statista, most of which should be encrypted. However Borgeaud also said that 40 percent of corporations reporting the state of data-at-rest said that only 21-40 percent of their data was encrypted last year. That indicates we have a long way to go before we solve the issue of secure data.

Cyber Protection Magazine has talked to more than 100 companies in the past two years that are dedicated to encrypting data in motion and data at rest. It is big business and there is no one leader in any of it that we can see in terms of revenue or technology. All of them claim to be profitable, so being first doesn't really mean a whole lot, but it doesn't make it easy for customers to make an informed choice. The best advice we can offer is to just pick a provider and hope for the best. Whatever the choice is will improve current security if you haven't had a provider before.

However, once the choice is made that doesn't solve the problem of data in use. That is the realm of a largely new security sector with the mouthful of a title: Fully Homomorphic Encryption (FHE).

Very simply, FHE encrypts data while a user is working on it, making it undecipherable even if a malicious actor has managed to infiltrate a network. Sounds pretty neat, but there are a couple of problems.

SLOW AND MASSIVE

First, encrypting data while in use slows down the computing time. Second, decrypting the data for use slows down computing time. Third encrypting data always tends to increase the amount of data making storage more expensive, especially using cloud storage. That limits what applications can actually use FHE. We count more than 20 companies engaged in FHE technology fighting for a very small amount of potential customers with limited budgets. One company we've talked to may have resolved all of those problems.

Datakrypto is a four-year-old start up that literally stumbled across their FHE solution while working on another problem, according to founder and CTO Luigi Caramico.

"Most FHE technology is impractical," he explained, "It slows compute time and increases data by a factor of 100,000. That would be like going to an ATM and having to wait five hours to get your money out."

Caramico claims their technology does increase the amount of data by about a factor of 1.5 or less, depending on how the customer wants to configure it, and increases latency by a few milliseconds.

Q-DAY PANIC

One factor the limits the adoption of encryption at any level is the fear regarding "Q-day". This is the moment when a quantum computer is manufactured, powerful enough to decrypt the most complex encryption in use today. Post quantum computing (PQC) is an industry sector dedicated to producing a new encryption standard that cannot be broken by quantum computers. FHE is related to this industry because it calls itself "quantum resistant."

Caramico dismisses that term, simply because he discounts the danger of quantum computing. "No one knows what quantum computing can do to encryption because no one has ever made a quantum computer powerful enough to accomplish the task." He has a point. Here are some hard numbers.

THE COST OF QUANTUM

A supercomputer, runs on 30 MWh or power. The most powerful quantum computer today capable of matching or exceeding the performance of a supercomputer consumes only 10-25 kWh. That alone justifies the investment in quantum.

However, the current cost per qbit, the measurement of compute power for quantum, is $10,000. The most powerful quantum computer in the world is around 1,100 qbits. To decrypt a single document requires a quantum computer with 20 million qbits. That makes the cost of the proposed system $200 billion.

The power that computer would consume is more than 125MW, but it also emits a tremendous amount of heat. That requires a cooling system keeping the facility at near absolute zero during operational hours. Such a facility needs an enormous continuous source of power, probably in the form of a nuclear power plant. That would $1.35 billion to the project total.

With this kind of cost and infrastructure is beyond the reach of ransomware gangs. It will have to be taken on by a nation-state with deep pockets. Even with all this, it would take that computer 8 hours to decrypt a single document. That makes it difficult to see an effective quantum computer capable of creating Q-Day, in our lifetimes.

That's why we recommend ignoring the fear, uncertainty, and doubt and just get to work encrypting all that data now.

LOU COVEY

Lou is Chief Editor of Cyber Protection Magazine

CONTRIBUTING AUTHORS:

Holly Burton

David Close

Brian Hill

Dwayne McDaniel

Christina Cravens

Tim Erlin

Rich Kanadjian

Subo Guha

Elisha Riedlinger

SPONSORS:

Special thanks to our sponsors for making this possible:

Safety National – safetynational.com

Lupasafe – lupasafe.com

EDITORS: Lou Covey & Patrick Boch

Issued by

CYBER PROTECTION MAGAZINE

www.cyberprotection-magazine.com

info@cyberprotection-magazine.com

What CIOs Should Prioritize

AUTHOR: ELISHA RIEDLINGER

The role of the CIO has certainly seen a dramatic transformation in recent years. The threats we're seeing today are nothing like what we faced even a year ago.

Here's what's keeping CIOs up at night: sophisticated attackers aren't even bothering with malware anymore. They're slipping past traditional security tools like they're not even there. Remember Volt Typhoon? I was working with customers as soon as Microsoft broke the news last year. CrowdStrike had just finished warning everyone at their RSA keynote about exactly this kind of threat. And yet, many companies are still scratching their heads about how to defend against malware-less attacks.

Legacy operational technology (OT) systems pose an even greater risk. These systems often run on outdated versions of Windows that are no longer supported. In today's geopolitical climate, this isn't merely an IT issue, it's a national security concern that directly impacts CIOs.

Interesting enough, some of the most effective security solutions have been with us all along.

While everyone has been fixated on sophisticated tools like Layer 7 firewalls, the basics—the foundational layers of the OSI model are frequently overlooked. Take proxies, for example. People dismiss them as outdated, but the core problem they were designed to solve hasn't gone away. Smart companies are dusting off these "old-school" approaches because the truth is…they still work. And now, more than ever, those neglected back doors are being targeted.

Programs like CTPAT (Customs Trade Partnership Against Terrorism) have existed for years, but suddenly, CIOs are scrambling. Why? Because the rules actually have teeth now. After all the post-2020 supply chain chaos—and with terrorism threats on the rise—companies can't just check boxes anymore. Compliance has to be meaningful, and that requires real implementation.

Then there's AI. I've saved this one for last because, frankly, it's still the Wild West. Sure, governments are starting to regulate AI weaponization, but for most organizations, AI isn't about building cool new tools—it's about figuring out how to defend against them. Let that sink in: we're not just protecting against human attackers anymore. We're now defending against machines that can think and adapt faster than we can.

For CIOs now attending RSA and looking to the future, this year is shaping up to be one of the most complex and challenging years yet. It's no longer just about keeping the lights on. They're tasked with modernizing outdated systems while adversaries grow more sophisticated. They're managing new compliance requirements in the face of rising nation-state attacks. And now, they have to figure out how to leverage AI—both as a defense mechanism and as a threat vector.

Add to that the financial impact of recent breaches—millions paid in ransom and losses reaching into the billions—and the stakes couldn't be higher. For many CIOs and CISOs, this is turning out to be the toughest year yet.

Meeting these challenges requires a balanced approach. You have to return to the basics, even as you look ahead to emerging threats. You can't afford to chase every shiny new tool, but you also can't afford to ignore innovation. The CIOs who sleep better at night will be the ones who find that balance—reinforcing the foundations while building a roadmap for what's next.

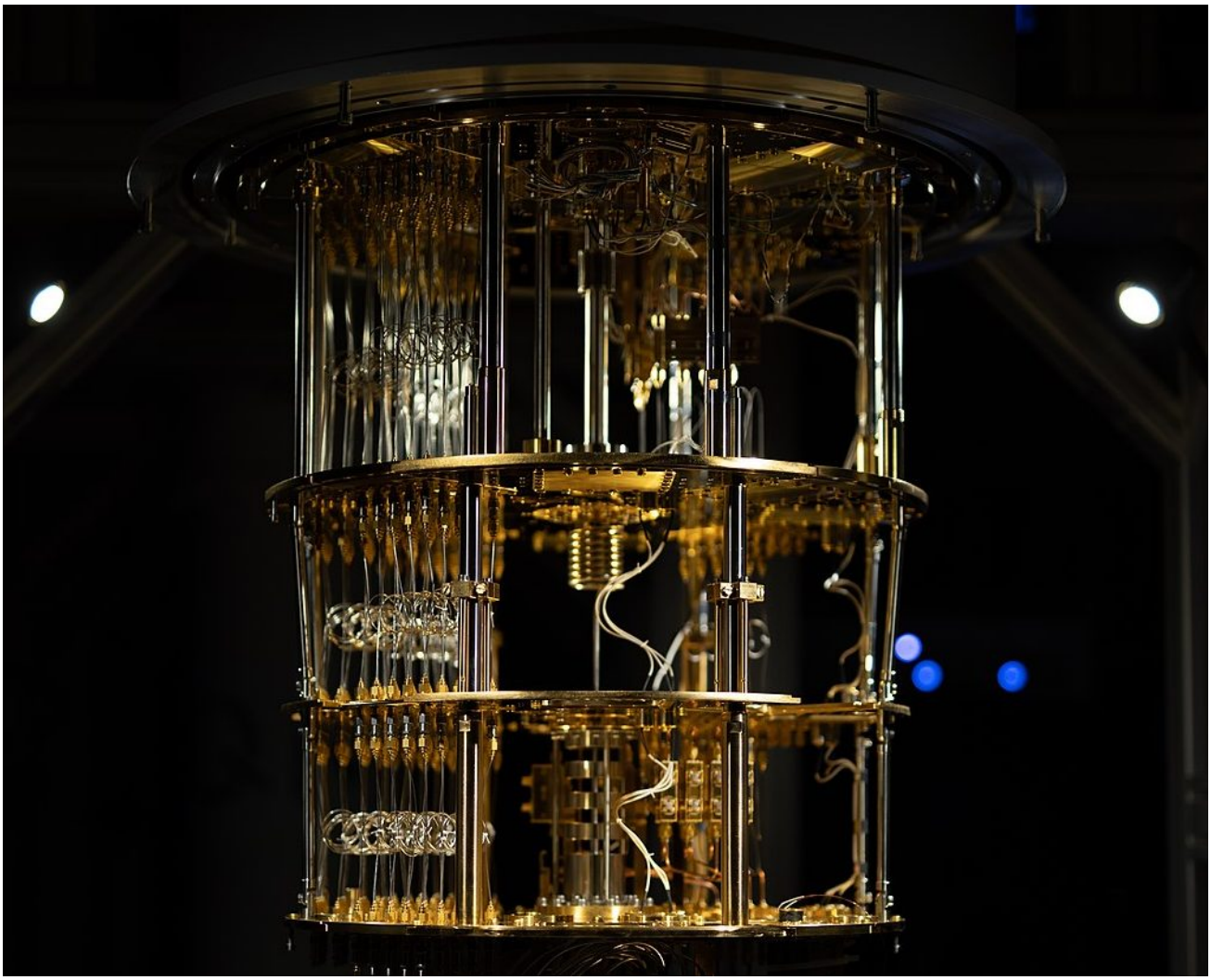
There may be no silver bullet, but one thing is clear: the playbook that protected us in the past won't suffice for the future. For CIOs, this is the time to re-evaluate old assumptions and invest in the principles that deliver long-term security.

ELISHA RIEDLINGER

COO at NeuShield

Post-Quantum Cryptography Event Horizon Approaches

AUTHOR: DAVID CLOSE



The rise of quantum computing poses a serious threat to current encryption methods. For decades, industries like banking, healthcare, and government have relied on encryption to protect sensitive data, whether in transit or at rest. However, as quantum computing advances, this lock is at risk of being picked. The question is not if but when quantum computers will render current encryption obsolete.

Quantum computers function as master lockpickers, capable of solving mathematical problems that traditional computers would take centuries to crack. This capability threatens the core of modern encryption, including widely used public key systems like RSA and ECC. When large-scale quantum computers become operational, bad actors can easily unravel public and private encryption systems. Everything from confidential patient records to

classified government communications could become vulnerable. While cybersecurity teams are already working overtime to patch vulnerabilities and prevent data breaches, quantum computing adds a complex new dimension to their challenges.

The Role of Post-Quantum Cryptography (PQC)

In response to these emerging threats, the National Institute of Standards and Technology (NIST) has finalized three post-quantum cryptography (PQC) standards in August 2024: 203-Kyber for lattice-based key encapsulation, 204-Dilithium for lattice-based digital signatures, and 205-SPHINCS+ for stateless hash-based digital signatures. These standards offer organizations a roadmap to future-proof encryption. Additionally, national initiatives, such as CISA's Post-Quantum Cryptography Initiative, spearhead efforts to ensure industries adopt quantum-safe solutions.

Among the quantum computing experts surveyed by the Global Risk Institute, 22.7% anticipate a quantum computer-based attack on RSA-2048 by 2030, while 50% consider it likely by 2035. The PQC market is projected to exceed $17 billion by 2034, underscoring the growing need for quantum-safe solutions. PQC algorithms, unlike traditional methods like RSA and ECC, leverage mathematical structures that quantum computers find significantly more challenging to solve, such as lattice-based and hash-based problems.

Key Action Steps

Conduct a comprehensive inventory of your cryptographic systems, protocols, and assets. Identify outdated algorithms, such as RSA and ECC, that are particularly vulnerable to quantum decryption. Prioritize systems handling sensitive, long-lived data.

Counter "Harvest Now, Decrypt Later" Threats

A significant quantum-era risk is the "Harvest Now, Decrypt Later" (HNDL) strategy, in which adversaries intercept and store encrypted data today to decrypt later using quantum capabilities. Secure data in transit with hybrid protocols combining classical and post-quantum encryption algorithms. For example, hybrid TLS implementations combining traditional encryption with CRYSTALS-Kyber offer immediate protection while paving the way for future transitions.

Code signing prevents quantum computing attacks by ensuring that only verified code runs on a system. By creating a quantum-safe signature, code signing prevents tampering. Why it matters: Code signing ensures software integrity and authenticity, guarding against tampering and malware injection. Without robust code signing, attackers can exploit critical software and firmware.

Legacy systems, including Industrial Control Systems (ICS) and other critical infrastructure, pose an additional challenge. Many rely on outdated cryptographic protocols and are not designed for seamless updates. Conduct a thorough assessment to determine their susceptibility to quantum attacks. Plan hardware replacement cycles that integrate quantum-safe cryptographic capabilities.

Building Long-Term Resilience

Organizations must adopt crypto-agile architectures to remain secure in an era of evolving cryptographic standards. Crypto-agility enables swift transitions between algorithms through centralized key management systems and software-defined cryptographic solutions. With these tools, organizations can deploy updates seamlessly, reducing downtime and maintaining operational security.

Hybrid cryptographic solutions combine classical algorithms with quantum-resistant alternatives. This transitional strategy ensures compatibility with existing infrastructure while preparing for quantum threats. For instance, applying a hybrid Certificate Authority (CA) solution combines conventional cryptographic signatures with PQC signatures, ensuring systems are compatible with current technology and secured against future quantum computer-based attacks.

Follow Standardization and Compliance

Keeping pace with emerging PQC standards is essential for long-term security. Aligning internal cryptographic practices with NIST standards ensures compliance with future regulatory requirements while bolstering organizational security. Adhering to industry best practices also fosters trust with stakeholders and partners in the quantum era.

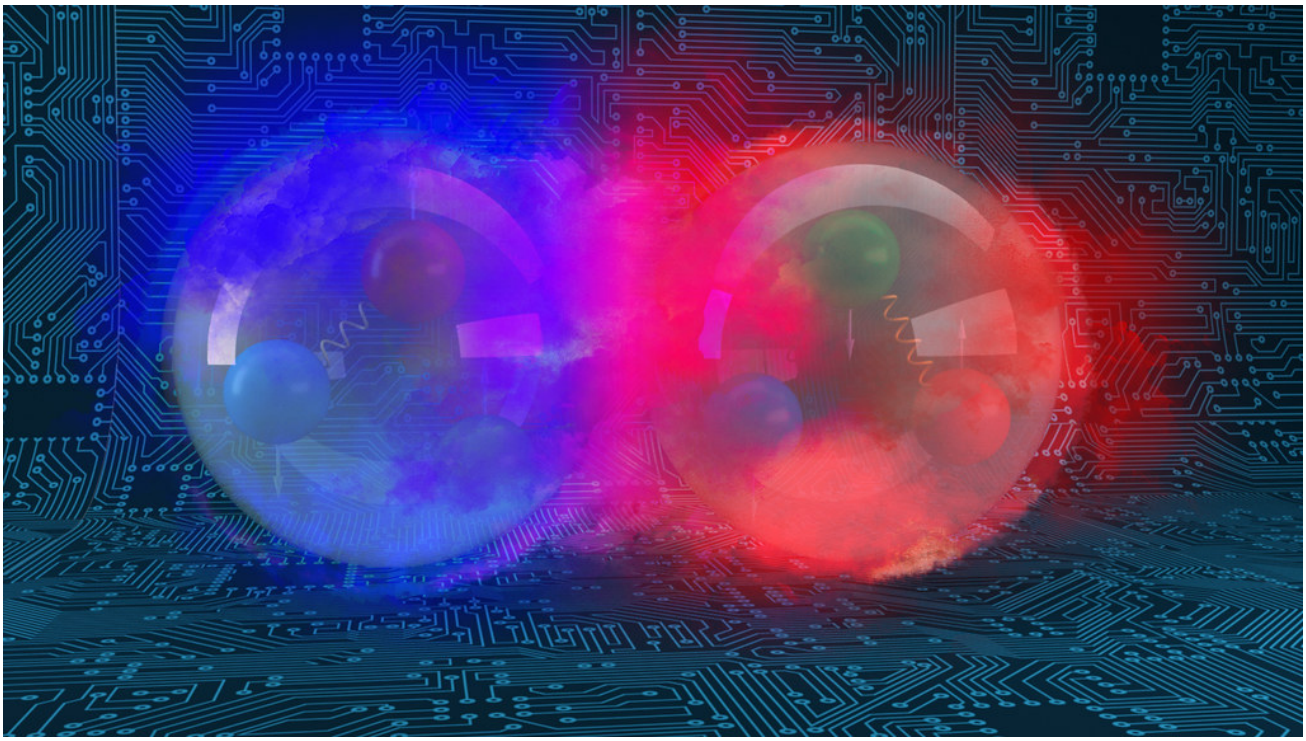
Organizations must develop a PQC strategy before their cryptographic infrastructure is compromised. By taking these proactive steps now, companies can prepare for the quantum future while maintaining security today.

DAVID CLOSE

Chief solutions architect at Futurex

Post-Quantum Readiness: A Strategic Imperative for Cybersecurity

AUTHOR: CHRISTINA CRAVENS



Quantum computing promises remarkable breakthroughs across science, medicine, and technology, but it also brings a looming threat to cybersecurity. The U.S. National Institute of Standards and Technology (NIST) has issued clear warnings: the encryption algorithms that protect today's data and communications could be rendered obsolete by the power of quantum computers. Once capable of breaking classical cryptography, quantum systems will put the confidentiality, integrity, and authenticity of digital assets at risk.

This is not a distant problem. Government agencies have begun to sound the alarm, encouraging public and private sector organizations to prepare for a post-quantum future now. The U.S. Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and NIST are urging companies to evaluate their current cryptographic posture and chart a path toward quantum resilience. But getting there requires more than just adopting a new set of algorithms.

Going Beyond Algorithm Swaps

"Post-quantum readiness" is not just a technical upgrade—it's a strategic, organization-wide effort. While new quantum-resistant encryption standards are being finalized, companies must begin preparing by developing a comprehensive understanding of how and where encryption is used within their

environment.

That includes building a full inventory of cryptographic protocols in use, mapping out encrypted data flows, and identifying dependencies across business systems. Many organizations are surprised to find that encryption is deeply embedded in everything from internal applications and cloud services to third-party integrations and legacy systems.

Understanding these dependencies is critical. Business functions that rely on encrypted communications – whether to secure customer data, authenticate users, or protect proprietary information – must be identified and assessed for quantum vulnerability. This level of visibility is the foundation of any meaningful post-quantum transition strategy.

A Looming Deadline for Visibility
The timeline for preparation is shrinking. Over the next year, businesses should create a detailed inventory of all cryptographic methods and encrypted data pathways that support critical business functions. This means knowing what algorithms are in use, where they're implemented, and how they tie into essential services and workflows.

Without this inventory, organizations will be unable to effectively prioritize their migration to post-quantum standards. Worse, they may be left exposed in areas that were overlooked, creating blind spots in otherwise mature security programs.

Building the Inventory
Creating this inventory doesn't have to be overwhelming. Modern approaches to cyber asset discovery can help accelerate the process. For example, network-based sensors that passively observe data flows can identify where encryption is in use and which systems are communicating securely. By layering in analytics and business context, these tools can help organizations correlate encrypted pathways to specific business functions and compliance requirements.

This kind of continuous, dynamic mapping – especially when supported by automation and AI – offers a scalable way to maintain up-to-date visibility as systems evolve and new technologies are adopted.

Preparing for the Transition
Once the cryptographic landscape is mapped, the real work begins. Organizations must evaluate which cryptographic implementations are quantum-vulnerable and start testing quantum-resistant alternatives. Not every system will need to be upgraded immediately, but those handling sensitive or long-lived data should be prioritized.

Ultimately, transitioning to post-quantum cryptography is not a one-time project. It will unfold over multiple years, requiring coordination across security, IT, compliance, and business teams. Organizations that start now, by developing cryptographic inventories and aligning their security programs with government guidance, will be in a much stronger position to protect their assets as the quantum era arrives.

CHRISTINA CRAVENS

Chief Growth Officer at Redjack

Hard to Hit a Shifting Target: Why Deterministic Approaches to NHI Security Are Flawed

AUTHOR: DWAYNE MCDANIEL

Stop me if you've heard this one. There's a classic joke in computer science: An engineer builds a bar and rigorously tests it out. First she orders 2 drinks, then 0 drinks, then -1 drinks, then she tries ordering a lizard, a NULLPTR, and even attempts to leave without paying and everything works as expected. When she opens shop the first real customer walks in and asks for the bathroom. The bar explodes.

The punchline isn't just a programmer's inside joke, it's a cautionary tale: even the most meticulously engineered systems can fail at the hands of real-world unpredictability. Nowhere is this more true than in the modern enterprise, where secrets sprawl, intimately bound to the proliferation of Non-Human Identities (NHIs), has become security's hardest-to-hit moving target.

Let's take a look at why solving for secrets sprawl with deterministic, rule based tooling is never going to be able to help team eradicate the epidemic of leaked plaintext credentials: an attacker's favorite way to move through your systems.

Secrets Sprawl: The Hidden Epidemic Behind NHIs

At first glance, defining non-human identities seems straightforward. It's just any entity that isn't a person but needs to access digital resources, such as service accounts, Kubernetes workloads, or IoT devices. However, how do you keep track of all of these

different entities? Unlike humans in your organization there is no formal onboarding, training, review or review being informed by HR.

But there is one thing they all have in common.

At the heart of all NHIs is their dependence on secrets: API keys, passwords, and certificates. These credentials are the lifeblood of automation and connectivity, but if not properly stored, rotated and eventually decommissioned, they introduce some serious risks for the organization.

Before you can think about automatically rotating these keys, you must first account for them. You need to find them all, properly store them and get your developers to stop adding them as plaintext to their code and collaboration tools. That last part is how NHIs go from an asset to a an attack path.

GitGuardian's 2025 State of Secrets Sprawl report underscores the scale and complexity of the problem. In 2024 alone, developers committed a staggering 23.7 million new hardcoded secrets to public GitHub repositories, a 25% increase from the previous year. Of what was found, 58% of these secrets were classified as "generic," up from 49% in 2023.

Generic vs Specific Secrets Detection

For a finite number of secrets, scanning services can build specific detectors, tailored to recognize credentials tied to known providers. Well known examples are keys with telltale prefixes like "sk-" for OpenAI or "gho_" for GitHub App tokens.
The credentials most NHIs use defy predictable patterns. Their forms are as varied as the systems they serve. These "generic" secrets, take the form of database connection strings, custom authentication tokens, and bespoke API keys and lack the standardized formatting that makes specific API keys easy to spot with pattern matching.

We already know the results when team members don't follow best practices. A tangled web of secrets scattered within codebases, configuration files, CI/CD pipelines, and cloud environments, many of them untraceable, unmonitored, and dangerously exposed.

Traditional, deterministic security tools search for known, well-defined patterns. This offers little protection against this diversity of secrets and leaves security teams with a dangerous blind spot.

The Way Forward: Adaptability Over Determinism

It's tempting to chase after every new secret format with ever-more-specific detectors, but history (and that exploding bar) teaches us that real-world complexity always outpaces what we can anticipate.

The answer isn't more deterministic rules; we need to invest in the foundational practices that limit secrets sprawl in the first place. This includes context-aware, intelligent detection tools that can let you:

- Build and maintain robust inventories: Know what NHIs exist, what secrets they possess, and where those secrets live.
- Ensure secrets management platforms are properly used: Centralize and automate how secrets are generated, stored, and rotated.
- Continually audit and monitor for new secrets: Don't just look for what you expect, keep watching for what you don't.

In a world defined by the unpredictability of NHIs and the relentless sprawl of secrets, security isn't about hitting a fixed target. It's about building resilient systems, fostering adaptable teams, and preparing for the surprises that always come with the next real customer, or attacker, walking through the door.

DWAYNE MCDANIEL

Developer Advocate at GitGuardian

Building a Better Security Analyst: What Humans Can Learn From AI

AUTHOR: SUBO GUHA

For AI to reach its potential, it requires significant up-front investment in knowledge training and briefing from human sources. The more knowledge humans take in fully training an AI model before it's deployed in a live environment, the more complex tasks AI can take on later. This is especially true of Agentic AI, which operates autonomously with little human intervention.

AI also holds great potential to be a powerful learning tool for humans. For example, security analysts in a security operations center (SOC) can tap into AI to learn new skills, brush up on existing ones, and keep pace with evolving cyber threats. AI tools for cybersecurity skills training can empower teams to improve how they detect and respond to threats with greater speed and accuracy. Let's look at some ways human security analysts can learn from AI.

Learning Through Automated Security Frameworks: It's now possible to train AI on specific cybersecurity frameworks such as MITRE ATT&CK, a globally accessible knowledge base of adversary tactics, techniques, and procedures (TTPs). Learning MITRE ATT&CK helps security professionals better understand how attackers behave and develop counter-defenses. By automating these TTPs and breaking them down into steps, AI can help any

security personnel, as well as other IT professionals improve their cybersecurity posture and be better prepared against adversaries.

Personalized Learning and Playbooks: AI can evaluate an analyst's current knowledge and create customized learning tracks based on their strengths, weaknesses, and current or desired role. AI agents can then create customized training playbooks that are tailored to an analyst's individual skill level using existing materials and their own training. These playbooks adapt as the analyst progresses and can be supplemented by AI chatbots and assistants for on-demand tutoring.

Threat Intelligence and Real-World Scenarios: AI can analyze data from attacks in the field and then generate dynamic threat simulations to help train security analysts to respond faster. AI-driven cyberattack simulations can mimic network breaches and other attacks, enabling analysts to practice responding to emerging threats and understand new attack vectors.

Automated Research and Skill Expansion: AI can easily summarize hundreds of pages of research and complex threat intelligence reports and NLP tools can track hacker activity at a faster rate than human analysts. They can recognize certain language patterns hackers use in social engineering hacks, and can even generate reports on these patterns for junior analysts.

Hands-On Coding and Automation: AI-powered coding assistants can help analysts learn various scripting skills for security automation and generate custom security scripts, improving efficiency and skill development. This helps analysts learn how to use security tools (e.g., Splunk, Wireshark, EDR platforms) by providing step-by-step guidance based on what the user is doing.

Security Gamification and Competitions: AI-powered agents can serve as tutors and create fun, personalized capture-the-flag (CTF) challenges that track performance in cybersecurity competitions and suggest areas for improvement.

Many in the security field have raised concerns that cybersecurity jobs may eventually become obsolete due to AI. The reality is, autonomous AI Agents and human analysts are much more interdependent. A well-built autonomous SOC will always need humans. The goal is to have mutual checks and balances, with human analysts always making the final call. While AI can do much more of the heavy lifting when it comes to detecting and analyzing threats, humans are essential to performing verification on the findings and conclusions drawn by AI. Organizations should see AI as a supplemental tool to optimize their cybersecurity efforts.

Optimizing the Human Experience

Human analysts and AI agents each have strengths and weaknesses. AI is better at analyzing and recognizing patterns and spotting anomalies in large datasets, and faster at writing scripts and code. Conversely, human analysts are better at making decisions based on their experience and understanding more nuanced situations. Humans can further train AI through feedback loops; each time an AI agent completes a task, the human can deliver feedback on how well it performed that task and how to do it better.

By integrating AI into learning, security analysts can accelerate skill development, stay ahead of threats, and become cybersecurity experts. Security practitioners need to find opportunities to close those AI skill gaps. Security professionals shouldn't be worried about job obsolescence due to AI. Instead, they should be concerned about missing out on job opportunities due to the lack of AI knowledge. It's now easier than ever for security analysts to upskill in AI.

Subo spearheads the development of Stellar's award-winning, AI-driven Open XDR solutions. With more than 25 years of experience, Subo has held senior leadership roles at industry-leading companies like SolarWinds, Dell, N-able, and CA Technologies.

SUBO GUHA

Senior Vice President Product Management at Stellar Cyber


Every 11 seconds a hacker
falls in love with your data*
CYBER PROTECTION
MAGAZINE
Protect your data
https://cyberprotection-magazine.com
*According to cybersecurity ventures