Insigniam QUARTERLY®

SIX | DATA PRIVACY AND SECURITY | By Scott Steinberg

Maintaining Security and Privacy Despite Disruption

Taking a **forward-thinking and proactive approach to cybersecurity** can help you better defend tomorrow's organization against rising digital dangers.

Cybercrime is today's fastest-growing form of criminal activity. McAfee reports that an average of 419 new high-tech threats are released every minute, and RiskIQ calls it at 648.With digital dangers costing organizations a whopping $1.8 million a minute in system downtime, brand damage and other response-related costs, 81% of organizations in a Cybereason study reported being extremely concerned about the possibility of such attacks.

One of the best-known examples is the May 2021 incident that hobbled America's Colonial Pipeline. Another is the December 9, 2021 discovery of a vulnerability in Apache Log4j, a Java library used by thousands of companies and software programs (knowingly or otherwise), which brought significant challenges for organizations in every field. Security researchers have since warned that hackers are making 100 attempts to exploit this security loophole every minute. >>>

$6.1T

The **estimated cost to global enterprises in 2021**, for ransomware attacks, now averaging one every 11 seconds. *Source: Cybercrime Ventures Annual Security Report*

While the average amount of time that malicious actors tend to go undetected in systems has recently shrunk, according to cyber-security firm FireEye's *M-Trends* 2021 annual threat report, companies still typically take 24 days to notice security breaches.

"The world of technology will be the next battleground on which many of the world's most meaningful conflicts will be fought," says **David Thomas, executive director of online programming** at the **University of Denver**. "Already, we're seeing many of the globe's largest and most powerful nations gearing up to engage in a new age of cyber warfare. Look closely, and you can already see the signs of a high-tech arms race taking shape."

A number of factors make it harder than ever to secure digital assets, and some of them, ironically, are brought on by organizations' own efforts to improve their information technology. "The more we go through digital transformation, which increases our reliance on data, and the more we focus on data management, the more imperative it becomes to protect informational assets," notes **Reza Morakabati, CIO** of data protection leader **Commvault**. "Organizations' threat surface is only becoming larger due to transformation and automation."

"The biggest challenge that organizations now face is that data is currently being exchanged across so many different online touchpoints," notes **Aaron Cockerill, Chief Strategy Officer for Lookout**. "Because everyone's moving to the cloud, and remote or virtual work solutions, there's effectively no fixed security perimeter [to watch over] anymore, and enterprises' visibility into what's happening in terms of data use and access is shrinking."

Open-source software presents another challenge, with Log4j alone used by enterprises in every field, across a multitude of programs from email services and web applications to cloud hosting platforms. Via open-source software solutions, virtual miscreants may already have access to more high-tech back doors than many realize. In fact, 90% of IT leaders are already using open-source software, knowingly or otherwise, according to Red Hat's 2021 *State of Enterprise Open Source Report*. These present potential vulnerabilities, as open-source programs are prone to errors, glitches and workarounds just like any other piece of software.

This means that, as a business, you should actively work to protect your back-end operations by engaging in automated software testing, code composition analysis (which checks underlying programs for loopholes and vulnerabilities), and workforce security education and skills training refreshes on a regular basis. And it's critical to have a step-by-step cyber threat response plan in place for any challenges that emerge.

419 to 648

The number of **new high-tech attacks** launched every minute. *Sources: McAfee and RiskIQ*

How to Fight Back

The odds are good that your business will, at some point, be virtually compromised—and as a leader, you cannot afford to let your organization face that possibility unprepared.

Some challenges may be internal: Human error is a leading source of security breaches. As important as it is to employ strong digital defenses, as Mr. Thomas notes, it's also important to provide your workforce with routine cybersecurity training and skills refreshes every six months.

"Developing a privacy-by-design culture and deploying digital countermeasures should not have us forget that the threat can also come from within," says **Insigniam partner Guillaume Pajeot**. "Who are the employees who have access to sensitive data and systems? Beware of subcontractors, trainees and temp personnel who could be working for various interests. And what

PREVIOUS SPREAD, DEMIO/GETTY IMAGES; ABOVE, QI YANG/GETTY IMAGES

about stakeholders who could release data to serve their cause? No policy nor system can respond to this kind of threat. It is all about relationship, listening and building cultures that spur trustworthiness and partnership across the system. There's no algorithm for these yet."

Mr. Thomas also advises investing in data management and risk mitigation services, which can sniff out the places where sensitive data resides in your business and help you quickly categorize it, secure it and cordon it off. It's not uncommon for information that's stored online or shared with networks or applications to accumulate in unexpected places through your business, or to go overlooked by your workforce for extended periods, presenting potential vulnerabilities.

a leading provider of enterprise-level secure access solutions. "In an age of distributed computing, where you cannot fully control access to devices and network connections, users' identity has become the new security perimeter."

Adopting a "privacy by design" mentality can also help you stay safer by fundamentally incorporating privacy into your product development and design processes, as Mr. Durand suggests. Privacy by design is a strategic concept that champions the interweaving of key privacy measures throughout the creation and operation of IT systems, networked devices, and organizational policies and procedures. In effect, it's an approach to systems engineering that encourages

"The world of technology will be the next battleground on which many of the world's most meaningful conflicts will be fought." —**David Thomas**, executive director, online programming, The University of Denver

An Updated Security Framework

Regardless of how advanced your IT solutions are, or how comprehensive your training, an organization can respond to threats more rapidly by adopting zero-trust security principles. Under the zero-trust operating framework, all high-tech network access and user communications are regularly authenticated and verified, and also consistently monitored for suspicious activity.

With zero trust, teams should be better able to identify and monitor possible unwanted points of high-tech entry, better control the flow of traffic coming in and out of networks, and—should threats arise—more effectively find ways to limit a cyberattack's potential blast radius. "We no longer live in a world where apps, data and users reside in a single location," says **Andre Durand**, **founder** and **CEO** of **Ping Identity**, you to integrate and apply end-to-end privacy-focused solutions from the earliest days of a design concept. Instituting it can also help prepare your enterprise for the demands of a technology-driven future.

For leaders, the to-do list is long but straightforward: The more you ingrain a mindset of healthy suspicion in your workforce; the more you use a multistep authentication process to verify uncommon or sensitive transactions; the more you impose need-to-know-basis account limits on access to information and networks as a fail-safe in the event of a breach; the more you keep tabs on data coming into or out of your apps and networks; and the more you leverage advanced high-tech tools to constantly scan for and predict cyberattacks before they strike, the more effective at defending against digital threats your organization will be. **IQ**34