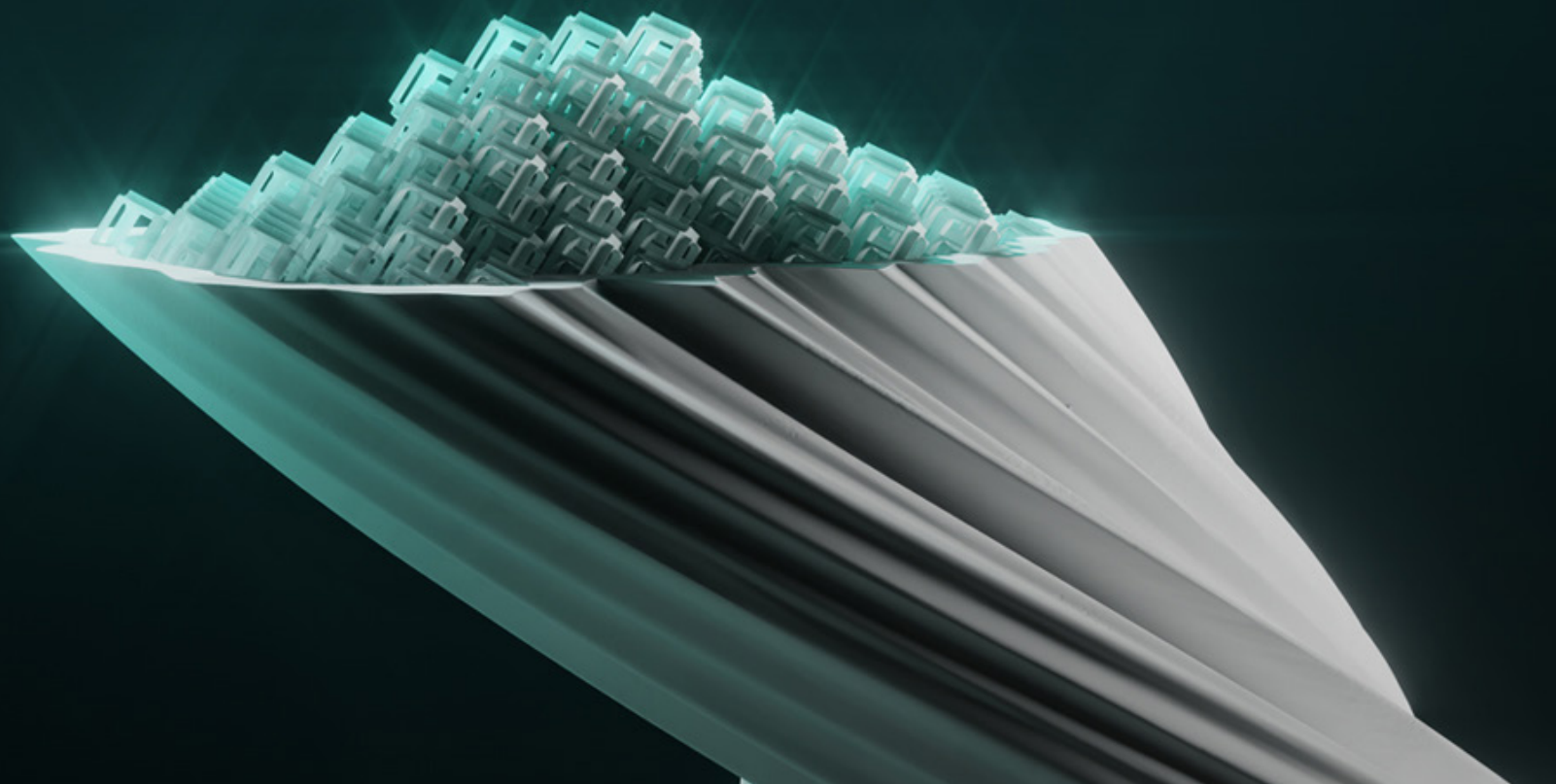
TOP FIVE SECURITY CHALLENGES FOR CISOs

What to look out for in the post-pandemic era



ESET®

Digital Security
Progress. Protected.

CISOs know that cybersecurity trends evolve relatively slowly from one year to the next. Rarely is there a lightning flash moment of cybercrime innovation that demands a radical rearchitecting of strategy. The pandemic changed this calculus completely.

Almost overnight, organizations were forced to radically overhaul business processes—to support mass home working and design new ways to reach their customers. At ESET we transitioned hundreds of employees to remote work in just days, battling VPN and cloud bottlenecks and device challenges in the process.

Unfortunately, in many cases these new digital investments and working practices created new opportunities for threat actors. Phishing volumes soared. Ransomware actors took advantage of vulnerabilities in VPNs and misconfigured RDP endpoints. Poorly secured cloud apps became a major focus for attack. The surge in threats told organizations what CISOs already knew—that prioritizing business continuity above all else comes with significant risks.

Source: ESET Threat Report T2, 2021

"With many still working from home, employees have gotten used to performing many administrative tasks electronically – and cybercriminals are taking advantage of this."

Jiří Kropáč

ESET Head of Threat Detection Labs

Source: ESET Threat Report T2, 2021

How to mitigate emerging risks?

Now we're emerging from the worst of the crisis, organizations must re-evaluate their risk appetite, and the balance between business operations and security. The hybrid workplace that most are adopting will be a more fluid, open environment than its pre-pandemic equivalent. For many, therefore, the focus should now be on risk mitigation that doesn't overly impact productivity.

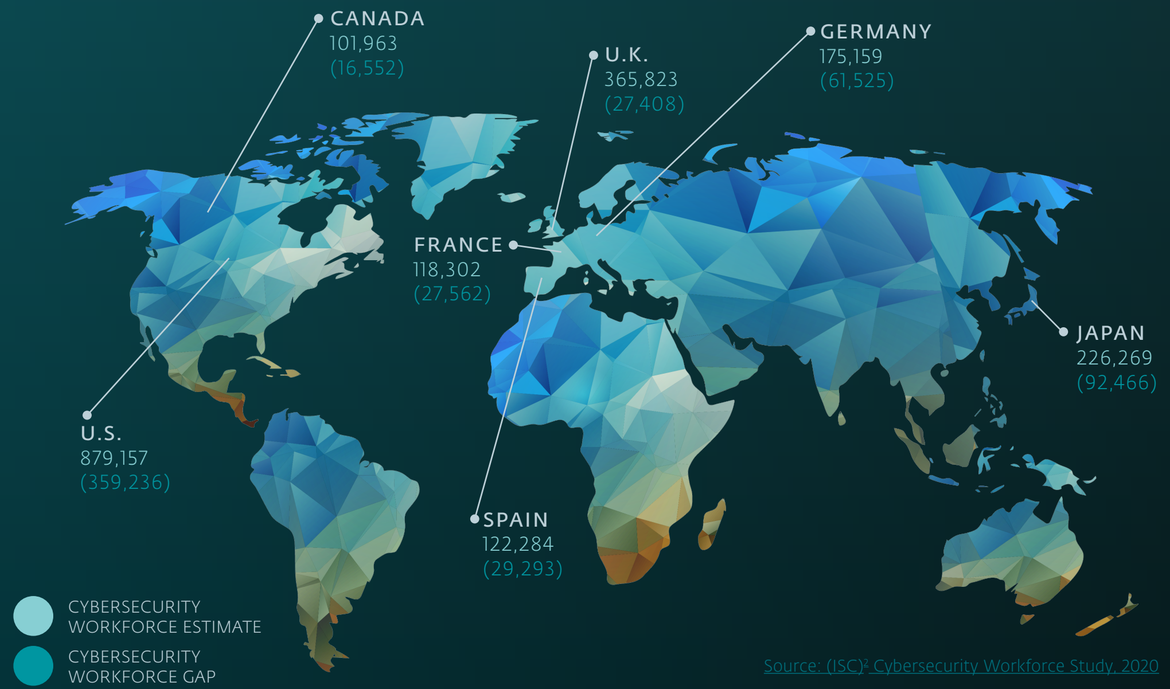
Fortunately, although organizations are undergoing yet another intense period of change, security best practices remain as valid today as they've ever been, while new approaches offer innovative solutions to emerging challenges. The following handbook will help CISOs to anticipate where risk might be most acute, and which measures can best mitigate it.

1. Tackling the great security skills shortage crisis

We all know it's getting harder to recruit security talent. Although the workforce gap closed for the first time in 2020, the global shortfall in skilled professionals still stands at over three million—including over 359,000 in the US. The rapid growth of cloud, IoT and other digital transformation projects has created a demand for security skills that far outpaces supply. As these investments continue in the post-pandemic era, skills shortages will become more acute, especially as older professionals retire. The need for cloud security talent is particularly great. The rise in misconfiguration incidents of late highlights the potential impact for firms.

Government plans to encourage more students into the industry are to be welcomed, but even if successful, they'll take years to have an impact. In the meantime, CISOs should try to leverage technology and outsourcing to mitigate the worst effects of skills risks. That means looking for machine learning and automation to take the leg work out of things like account management, policy optimization, code audits, and threat detection and response. On the latter, a growing range of managed detection and response (MDR) services offer CISOs new opportunities to hand over responsibility for operating EDR and XDR solutions. That not only helps to alleviate skills challenges but puts these capabilities in the hands of trained experts, who can also bring their expertise and industry-wide insight to bear.

Global Security Workforce and Gap Estimates



Source: (ISC)² Cybersecurity Workforce Study, 2020

IT companies also have a role to play. By creating IT hubs, education programs, and other outreach activities, including volunteering (as many ESET employees do), they can help to drive awareness of security and interest in it among school-aged students.

67% of business leaders understand the importance of security in remote work environments. Lack of leadership awareness has a real impact on teams.

Source: (ISC)² Cybersecurity Workforce Study, 2020

2. Managing third-party risk

Supply chains have come under close scrutiny during the pandemic. This is a good thing. In fact, they've been taken for granted by many businesses, to the point where many aren't even sure how many external suppliers they use to provide essential products and services. Unfortunately, those contracting for your organization may also represent a major cyber risk, especially if they're allowed access to corporate networks and resources. A 2018 study found that negligent insiders and contractors are considered the weakest link in the security chain—potentially responsible for data breaches, phishing attacks and ransomware compromises. Compounding the problem is the fact that contractors often aren't included in staff security training and awareness programs.

CISOs ideally want their suppliers to have the same or better level of security as their own organization. To achieve this requires continuous assessment, perhaps based on questionnaires developed from internal policies and standards. Vendor certifications can also provide useful insight into controls adoption and some can be automatically evaluated. In fact, automation is helpful throughout via Vendor Risk Management (VRM) tools, to check open data and estimate supplier security posture in various areas. Some vendors even run private honeypots to check for attacks. Organizations must first ask themselves what their priorities are with VRM and, based on these answers, develop strategy accordingly.

Digital Security
Progress. Protected.

Source: Microsoft 2021

3. The new reality of the hybrid workplace

Hybrid working is a chance to have the best of both worlds—meeting new employee expectations around work-life balance while driving innovation through face-to-face interactions. Yet it also exposes organizations to the risks associated with remote working: distracted users, unpatched endpoints and remote access infrastructure, weak account passwords and cloud misconfigurations. Plus, there's an elevated threat of lost/stolen devices, shoulder surfing and unsecured Wi-Fi networks impacting employees as they travel again.

CISOs should revisit corporate security policy with an eye on this new landscape. That could mean rolling out MFA, tighter access controls and micro-segmentation as part of a Zero Trust push. It could also mean outsourcing threat detection and response via MDR, and building new employee awareness and training courses. Most importantly, it will involve a blend of people, processes, and technology based on best practices, like those listed on the right.

READ MORE ON HOW TO SECURE YOUR REMOTE WORKFORCE.

Source: NCSC, 2021

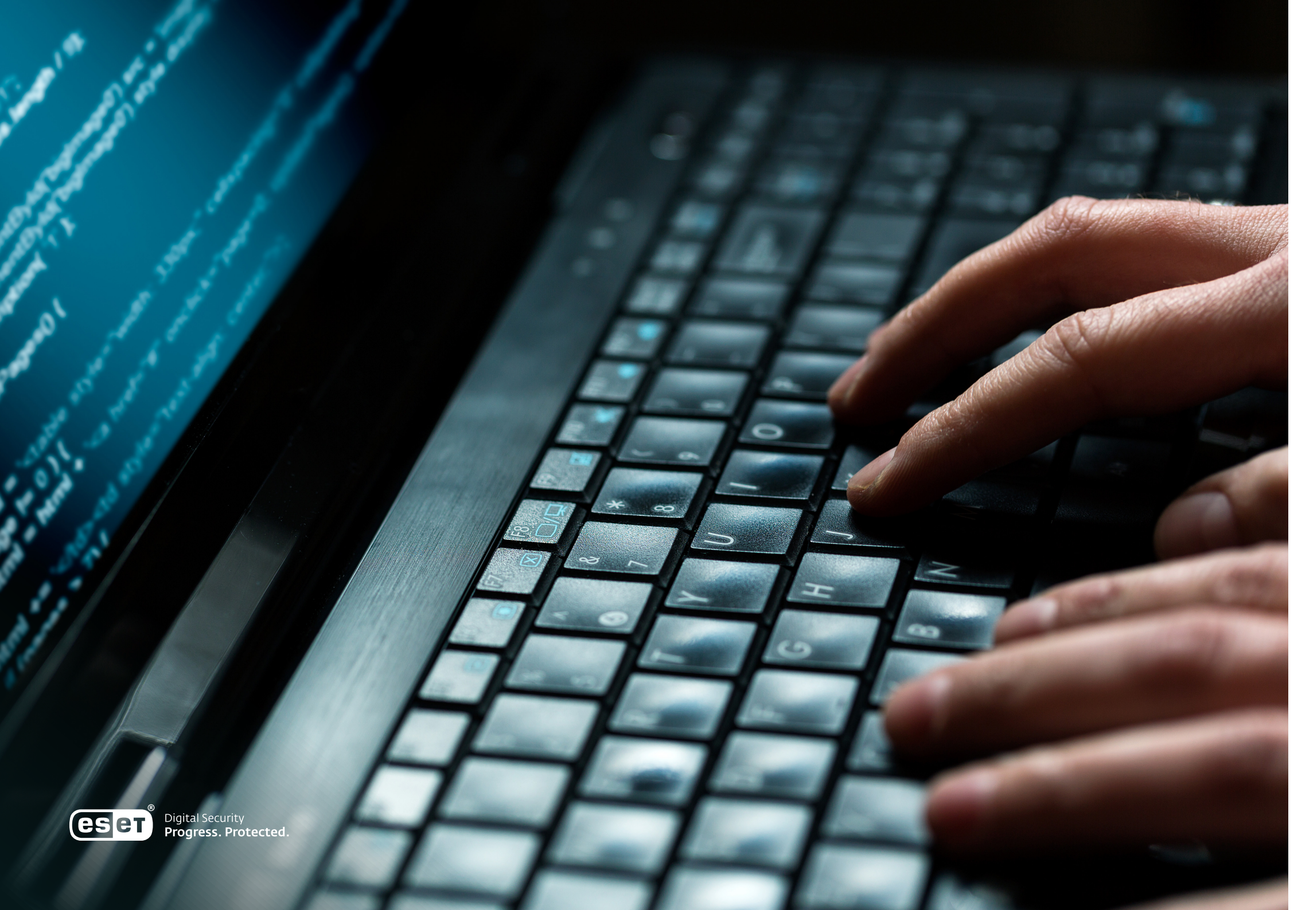
4. Consider a Zero Trust approach

The hybrid workplace will be one characterized by BYOD, hybrid cloud environments and regular movement of employees in and out of the traditional corporate perimeter. That kind of complexity is incredibly challenging to manage whilst maintaining productivity and a seamless user experience. This is what Zero Trust was built for. First described over a decade ago, it's predicated on a notion of "never trust, always verify" in order to reduce the impact of breaches. That means treating all networks as untrusted and continuously authenticating users and devices; enforcing the principle of least privilege; and assuming you've already been breached.

The good news is that many of the steps required to drive Zero Trust—like multi-factor authentication, micro-segmentation, EDR, host-based firewalls, data encryption and vulnerability management—may already be part of your set-up.

Key areas in which CISOs can take action

Source: Brian Kime, Forrester – senior analyst and guest speaker at ESET World



5. It's time for proactive security

CISOs instinctively understand that mitigating cyber risk is cheaper and easier when done ahead of time, via proactive measures. The challenge is in finding enough resources and knowing where to focus them, in order to get the best value. The scale of the challenge seems overwhelming.

Pen-testing offers a useful way to find exploitable vulnerabilities in the organization and can help to prioritize patching efforts, although a lack of integration with these tools into development/operational processes can slow the speed of remediation. Automated, risk-based patching solutions are best, to help organizations prioritize the huge number of CVEs they're flooded with each week.

Another step is to deploy EDR and XDR, to proactively and rapidly identify covert threats through correlation and analytics that uncover activity which human eyes may miss. There's some useful advice here. As for misconfiguration—data encryption, automated policy configuration checks early in the development lifecycle, and continuous auditing via Cloud Security Posture Management (CSPM) tools can all help to mitigate the risks.

Above all, as your organization continues to change and its business model evolves, it's important to ensure that security strategy and culture keep pace. That means not only deploying additional controls and expanding the function itself as the IT environment becomes larger and more complex, but also formalizing processes via a proper governance framework. That's the kind of organizational maturity your business may need, and CISOs should focus on, as it hits a new period of post-pandemic growth.

Over 18,000 CVEs

were disclosed in 2020 – more than in any other year.

Over 7 billion breached records

in 2019 were down to preventable configuration errors.

Source: Redscan NIST Vulnerability Analysis, 2020

LOOKING TO SET OFF ON THE RIGHT FOOT WITH ENDPOINT DETECTION AND RESPONSE?

ESET EDR provides outstanding visibility and synchronized remediation

LEARN MORE

eset Digital Security
Progress. Protected.

For over 30 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted.

Digital Security
Progress. Protected.