DocuSign

eBook

8 Security Trends Shaping the CISO Agenda Today

For CISOs, balancing day-to-day security operations with strategic planning becomes more challenging every day. Factors from remote work, cloud and Internet of Things (IoT) to application programming interfaces (APIs) and cloud-native development lead to an ever-expanding and diversifying attack surface—which in turn calls for proliferating security technologies. Innovation by both businesses and cybercriminals brings new types of risks and threats. Rapidly changing workforce models call for new ways to protect people and data in more places without impeding productivity or satisfaction. Regulatory changes and threat alerts make it hard for CISOs to get out of reactive mode for higher-level proactive thinking. Meanwhile, the drive for cost optimization and the cybersecurity talent shortage remain as challenging as ever.

Amid these competing pressures and priorities, eight security trends stand out as particularly significant for guiding the CISO agenda.

DocuSign

1/ Artificial intelligence is transforming enterprise security

Artificial intelligence has quickly become top-of-mind throughout today's executive suite, and the CISO's office is no exception. In some ways, the rapid advance of AI and machine learning is a welcome development. With human talent in short supply, these technologies are ready and willing to do their part for enterprise security. Already widely used in anomaly detection, AI-powered tools are expected to become even more prevalent, including areas such as identity and access management (IAM), monitoring, resource and threat analysis and rapid response. Trained experts are already using AI to detect vulnerable code and automate security tasks.

On the other hand, AI can also introduce new risks—especially in the hands of users eager to try out new use cases. Developers have been quick to embrace the ability of large language models (LLMs) like ChatGPT to write code, for example, but given its lack of built-in knowledge of development concepts and contexts, the tool can easily generate code with severe security vulnerabilities. When these flaws end up being introduced into the production environment, they're all too easily exploited by malicious actors.

The risks of AI aren't limited to coding. One survey found that 100% of SOC respondents want to use unsanctioned AI tools to work more easily, efficiently and/or effectively. But as with any shadow IT, this practice can undermine security and leave company systems and data exposed to unknown third parties. Employees using ChatGPT to summarize meeting notes, engineers using it to optimize code or salespeople using it to generate customer proposals are likely unaware that LLMs can use this data to train the algorithm and include confidential corporate data verbatim in future responses.

CISOs need to move quickly and thoughtfully to implement policies governing the use of AI and LLMs across the enterprise. At a minimum, these should include:

- Prohibiting the use of unsanctioned AI tools
- Prohibiting entering sensitive information into any public-facing LLM
- Including LLMs in standard confidentiality agreements

DocuSign

2/ Ransomware is growing more widespread—and easier than ever to launch

Ransomware remains as serious a threat as ever—and the worst is yet to come. Recent incidents show the vast scale of the threat:

MGM Resorts International (September 2023)

A cyberattack caused the Las Vegas-based company to shut down casino and hotel computer systems for ten days, costing the company an estimated $100 million.

City of Oakland (February 2022)

A far-reaching attack on systems holding data about payments, permits and licensing led the city's leadership to declare a state of emergency. Roughly 600 GB of sensitive personal information was subsequently released on the dark web.

MediaMarkt (November 2021)

Europe's largest consumer electronics retailer faced a $240 million ransom demand to recover encrypted files and restore retail store operations.

Kaseya (July 2021)

Between 800 and 1,500 of the managed service provider's customers were affected by an attack perpetrated by the Russia-based REvil group.

JBS (May 2021)

The world's largest meat producer was forced to shut down all of its U.S. plants—responsible for nearly a quarter of American supplies.

Colonial Pipeline (May 2021)

Facing the disruption of nearly half of the fuel supply for the U.S. East Coast, the company had no choice but to pay $4.4 million for a tool to reverse its ransomware encryption.

Large enterprises are focusing more on ransomware defense, but cybercriminals are working just as hard to stay one step ahead. They're finding ways to breach standard multifactor authentication (MFA) and using supply chain attacks to circumvent enterprise security. They're targeting more vulnerable small and mid-size to large institutions, with less focus on larger national infrastructure targets. They're expanding the platforms they target, including the Linux systems used in cloud and virtualization, and going after newer technologies like IoT and autonomous vehicles with more bugs and less protection.

They're now using AI as well. AI-powered ransomware can mimic normal system behaviors to evade detection, while ChatGPT is making it easier than ever to author ransomware malware as well as the phishing emails used to launch an attack.

In a particularly insidious twist, as companies protect themselves with cyber insurance, they become more likely to be targeted based on the size of their coverage, which criminals make a point of discovering.

In response, CISOs need to redouble efforts across every element of ransomware defense, including user education, anti-phishing training and malware detection—especially tools using AI/ML, endpoint detection & response (EDR), data protection and rapid recovery solutions. Zero Trust best practices remain an essential element of any modern security strategy.

DocuSign

3/ Application security is being reshaped by cloud-native development

Modern businesses run on applications. Customer-facing apps provide services, enable transactions and deliver streaming content. Partner and supplier apps interconnect supply chains and sales channels. Internal apps let employees access tools and resources wherever they work. All of these apps and their data are susceptible to hacking, zero-day attacks and identity theft—driving a booming market for application security that's been projected to surpass $7.5 billion.

At the same time, the rise of cloud-native development is changing the way companies approach AppSec. To accelerate time-to-market and increase business agility, teams now use methodologies like DevOps, Agile and CI/CD to assemble apps quickly using microservices and APIs. Delivered via the cloud, they can reach users more flexibly and scale more easily while yielding significant cost advantages. It's no wonder that Gartner predicts 95% of new digital workloads will be deployed on cloud-native platforms by 2025.

For CISOs, the challenge is to strengthen AppSec without sacrificing the benefits of cloud-native development. A key approach to achieve this is DevSecOps, an AppDev approach that emphasizes security throughout the software development lifecycle, from planning and design to testing and deployment. In the spirit of shift-left development, DevSecOps makes it possible to identify and address security issues earlier in the development process when they're easier and less costly to fix, as well as helping to prevent security vulnerabilities from reaching production.

API security now plays a critical role as well. The plumbing of cloud-native apps, APIs connect microservices throughout the enterprise and with third parties—but if not properly secured, they can provide a point of entry for attackers. API security technologies such as Secure API gateways help control access through authentication and authorization, encryption and monitoring.

DevSecOps and API security should now be top priorities for every organization.

4/ Cloud-based data breaches are bringing identity to the forefront

Driven in part by the pandemic, which led companies to seek greater agility, flexibility and scalability, cloud migration is booming. As the volume of cloud data increases, so does the risk of cybercrime and unauthorized access—as CISOs are well aware. In the 2022 Thales Cloud Security Report, 45% of businesses had experienced a cloud-based data breach or failed an audit in the past 12 months, while the 2022 Check Point Cloud Security Report found that 27% of organizations have experienced a security incident in their public cloud infrastructure within the last 12 months.

Fortunately, cloud security spending is booming as well. According to Statista, cloud security is the fastest-growing segment in the IT security market, with an estimated growth of nearly 27% from 2022 to 2023. This investment shows that companies understand their essential role in the security of their cloud data. Under the shared security model, cloud vendors provide secure infrastructure, including hardware, software, networking and storage, but their customers are responsible for securing their own data, apps, OS and configurations.

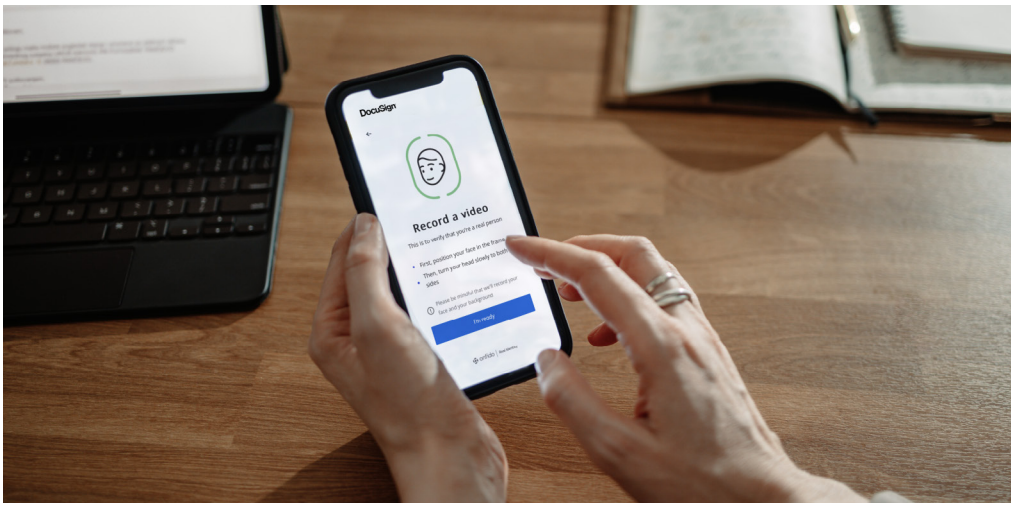
Together with fundamentals like encryption and monitoring, companies are now increasing their focus on identity as the foundation of data security. Encompassing complementary technologies including Identity and Access Management (IAM), Identity Governance and Administration (IGA) and Privileged Access Management (PAM), identity security seeks to ensure that only authorized users have access to sensitive data and applications and that access is restricted based on the user's role and level of authorization. Complementary tools such as Cloud Infrastructure Entitlement Management (CIEM) and Cloud Access Security Broker (CASB) allow greater visibility and a better understanding of risks and vulnerabilities in the environment by discovering and controlling which users and systems have access to what resources across cloud and hybrid infrastructure.

Here again, Zero Trust remains essential. By enforcing the principle of least privilege and applying network micro-segmentation, companies can limit access and movement as strictly as possible within the context of real-time access needs.

CISOs shouldn't let security concerns stand in the way of the real business benefits of cloud, but the security of these resources must be approached with the same rigor as on-premises environments.

DocuSign

5/ Mobile threats are on the rise—and so are privacy concerns



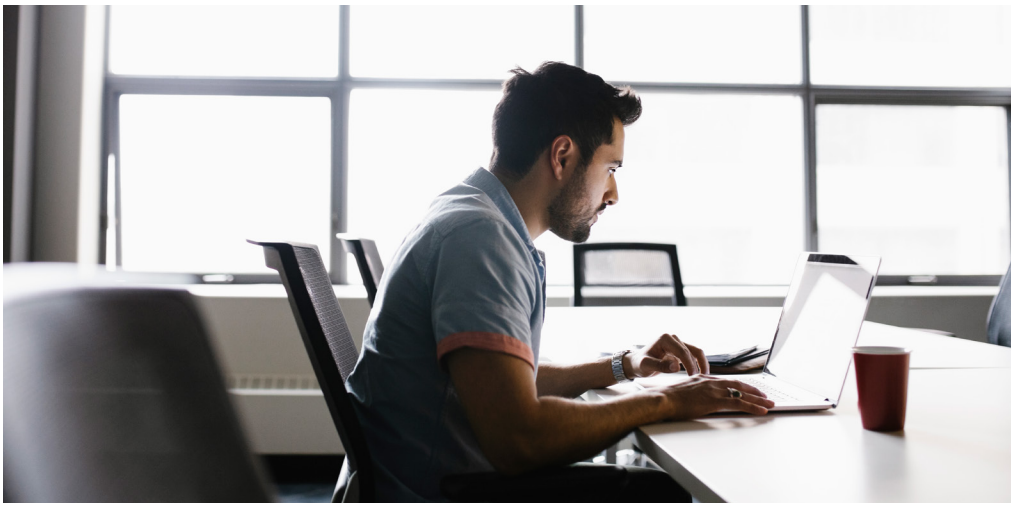
Employee-owned devices have been a fact of life for businesses for many years, but the risks they pose are now increasing. As people use the same devices for work and personal life, they end up with a mix of personal and business information on their laptops, smartphones and tablets. This can lead to sensitive business data being exposed to malware through the usage of unsafe consumer cloud services, apps and mobile sites. Ads by "malvertizers" are loaded with viruses, malware and Trojans that can create openings for hackers to enter. Meanwhile, the IoT is connecting everything from digital wallets to home security systems to cars—and IoT devices are notoriously under-protected.

Meanwhile, mobile malware is on the rise. A recent Proofpoint report found that detected mobile malware attacks spiked 500% in the first few months of 2022. Check Point's 2022 Cyber Attack Trends Report notes that 12% of corporate networks have been attacked using mobile vectors.

Some countermeasures to these mobile threats are straightforward and familiar, such as multifactor authentication (MFA), encryption, firewalls, anti-malware software and employee education. But one cornerstone of enterprise security poses particular challenges in mobile: knowing where data is stored and who has access to it. In a corporate environment, this can be achieved by implementing data classification policies and monitoring data access—but such measures raise privacy issues when applied on personal devices.

One way to reduce the vulnerabilities posed by BYOD mobile devices is for CISOs to use mobile application management (MAM) tools to manage corporate apps on employee-owned devices without disrupting their personal apps or data. Mobile threat detection can help security teams respond quickly to incidents, while cloud access security broker (CASB), VPN and secure gateways will help protect data wherever employees connect.

6/ Supply chain attacks call for third-party risk management



Security is only as effective as its weakest point; even the most sophisticated enterprise defenses can be undermined by gaps elsewhere in the supply chain. In fact, cybercriminals often target smaller supply chain organizations and third-party apps that might have access to the same information as their larger partners but don't have an equal level of protection. In 2023, Progress Software's MOVEit vulnerability led to a gigantic chain of record-breaking breaches. TechCrunch has reported that this single vulnerability cost businesses over $9.9 billion, with over 1000 businesses and over 60 million individuals affected.

Failure to assess this type of third-party risk exposes an organization to supply chain attacks, data breaches and reputational damage. Supply chain attacks quadrupled in 2021, while Gartner predicts that by 2025, 45% of organizations will experience attacks on their software supply chains—three times as many as in 2021.

In response, regulators globally are introducing new laws to make vendor risk management a priority. Boards and CEOs are already demanding security improvements in their supply chains such as demanding higher levels of compliance specificity and aggressively enhancing existing rules. A growing market for third-party risk management (TPRM) solutions and services enables organizations to monitor and assess the risk posed by third parties to make risk-informed decisions and reduce the risk to an acceptable level.

CISOs need to ensure they're up to speed on the latest tools, services and vendor questionnaires to help catalog and monitor cyber risks in third parties and suppliers. Best practices to manage third-party risk include:

- Know who your third parties are and understand exactly how much is being shared with each
- Prioritize vendors based on the level of risk they pose
- Monitor vendors continuously and automatically
- Collect consistent data across all to compare and contrast risks

7/ Human-centric security design is strengthening user awareness

The human element has always been targeted in cybersecurity. Even today, employees are notorious for poor online hygiene, weak passwords, unsafe browsing and circumventing security controls perceived as intrusive or cumbersome. They fall behind on security training, neglect security policies and fall prey to social engineering and phishing attacks. Addressing this vulnerability is both urgent and extremely challenging.

CISOs are now turning to human-centric security design to make people more willing, likely and able to manage their own security effectively. Prioritizing the role of employee experience—not just technology—across the controls management life cycle, this approach puts people at the center and realigns existing security approaches around them. Drawing on principles from behavioral sciences, user experience and related disciplines, organizations model how real people interact within data and asset workflows and processes, then tailor their security products to minimize unsecure behavior in intuitive and unobtrusive ways. According to Gartner, by 2027, 50% of large enterprise CISOs will have adopted human-centric security design practices to minimize cybersecurity-induced friction and maximize control adoption.

Steps to implement human-centric security design include:

- Assess your current cybersecurity posture to identify vulnerable points
- Test employee awareness
- Create a prioritized list of the types of risks each individual would experience
- Promote critical thinking and awareness among employees
- Invest in progressive policies that help influence positive security behavior, including regular training to improve decision-making

8/ Enhanced people management can help CISOs build a deeper cybersecurity team

Staffing remains a perennial challenge for CISOs desperate to attract and retain skilled experts. Human-centric people management can help. Working in tandem with a strategy-focused HR team, CISOs can take a structured, organizational approach to design and deliver a better talent experience—not just one-off initiatives and feel-good policies. Gartner reports that "CISOs who take a human-centric talent management approach to attract and retain talent have seen improvements in their functional and technical maturity."

Tactics for human-centric people management focus on creating a more rewarding experience for employees while also driving business outcomes. CISOs should help their team members gain new skills to advance their careers and find opportunities for internal advancement. Along similar lines, employees should be encouraged to participate in open-source projects, author articles/blogs and pursue industry speaking opportunities to raise their professional profile. Internal mentoring programs can help employees build their skills and strengthen retention. Allowing employees to dedicate time to new projects and experimentation encourages innovation while improving engagement and satisfaction.

Read more about how to protect your organization in our recent blog post, Innovative Organizations Need to Invest in Security Tools to Protect Valuable Data.

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
Visit www.docusign.com
Call +1-877-720-2040

DocuSign®