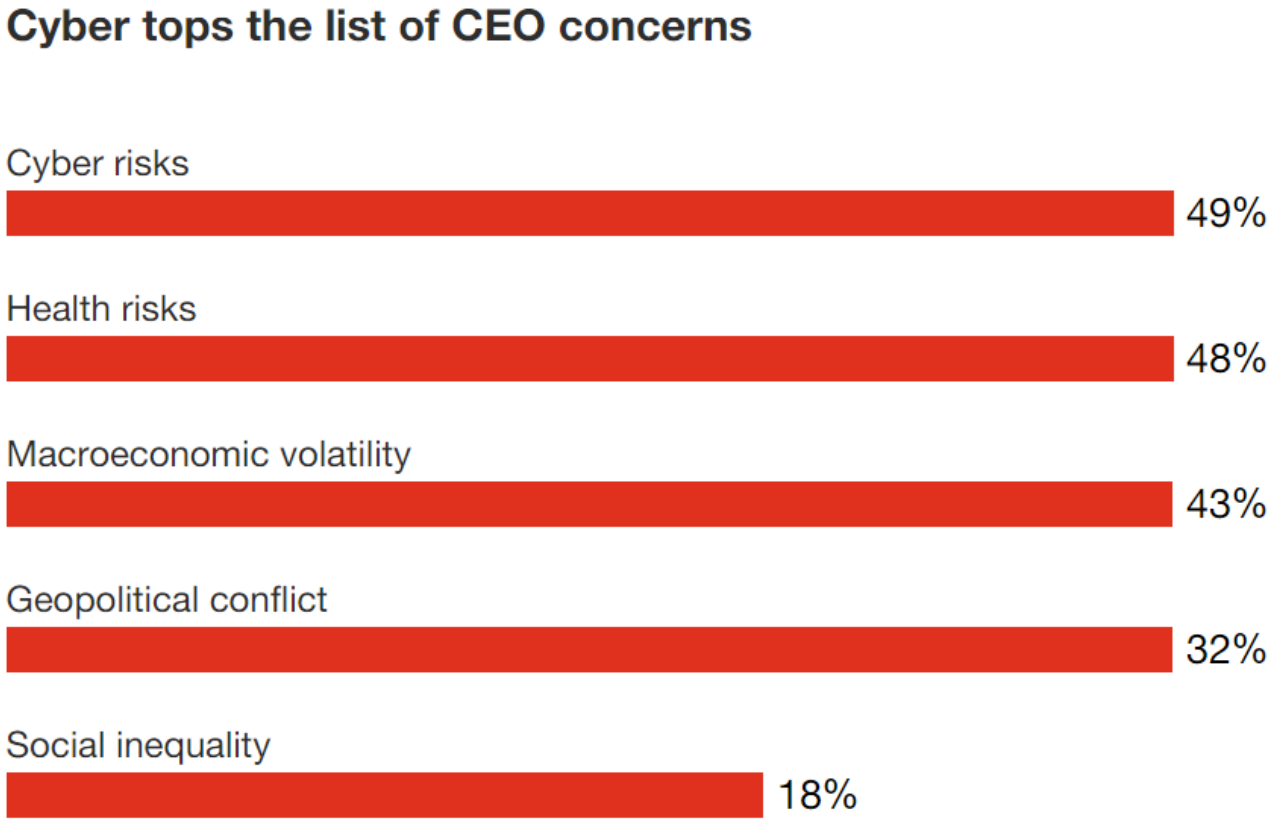
Cyber threats: What the C-suite and boards need to know and act upon

Sep 2022

Cybersecurity: Top of the list of CEO Concern

There remains a certain mystique around cybersecurity, due to the fact that much of the work involved–both successful and unsuccessful–is invisible to those not in the field. But with businesses digitally connecting more processes, products and people, cybersecurity risk has risen to the top of the list of CEO worries globally.

Our analysis in this report is based on intelligence gleaned from PwC's incident response engagements and our managed security operations services around the world. It's founded on in-house intelligence on cyber attacks and a wide variety of threat actors.



Question: How concerned are you about the following global threats negatively impacting your company over the next 12 months? (Showing only "very concerned" or "extremely concerned"' responses)
Source: PwC, 25th Annual Global CEO Survey, January 2022.

Four cyber threat trends

- Ransomware
- Supply chain compromise
- Discovery and Disclosure
- Cyber attack at scale

Ransomware

Ransomware dominated the headlines in 2021 as the data of 2,435 victims was exposed on leak sites, almost double the 1,300 victims in 2020. Threats multiplied, their sophistication increased and ransom demands climbed.

Scalability. Ransomware operations now run as businesses, with the main operator entering agreements with affiliates to "lease" the ransomware.

Fewer skills required. Attackers can rely on an established cybercrime ecosystem servicing ransomware operations, including access-as-a-service operations and credentials marketplaces, but remain independent of them.

Profitability. High-profile ransomware attacks in 2021 have seen victim organizations paying seven-figure ransoms.

Ransomware

Takeaways

For boards. Acting quickly can prevent widespread impact. Conduct regular **crisis simulations**, **from the board level down to security operations**, so everyone can have a chance to rehearse what to do if ransomware strikes

For the CRO and Business heads
CROs: Review your **cyber insurance** plan. Will it be adequate to **cover potential costs** for ransomware payment and recovery? Do you need to consider alternatives? How would a ransomware incident **impact revenues and financial reporting**? What is your responsibility for **investor disclosure** if there were a material impact?
Business heads: Review your **business continuity plans** to ensure critical business services are not disrupted if your mission-critical digital assets are compromised

For the CIO and CISO: Implement an **intel-led approach** to hygiene and **threat detection** to track known ransomware threat actors and their tools and methods and stop them.
Build **partnerships** with national and local government agencies tasked with cyber defense. Be prepared to **share information.**

Supply chain compromise

Supply chain compromises became commonplace in 2021. Attacks took several forms: software attacks, digital trust compromises, abuse of trusted infrastructure and third-party access.

Supply chain attacks have long been used by multiple threat actors. While they're traditionally associated with state-sponsored threat actors, financially motivated threat actors have become very successful in exploiting them.

Takeaways

For boards. What steps is management taking to implement **Zero Trust** principles? (The Zero Trust security model assumes that your systems have already been breached. This requires evolving the security mindset and controls from the traditional philosophy of **"trust, but verify" approach to "never trust, always verify."**)

Consider **consolidating** your tech vendors/supply chain to **reduce complexity**. It can be helpful to ask management what plans they have for **uncovering blind spots in your business relationships** that could have an impact on risk.

Supply chain compromise

Takeaways

For the CRO and Business heads
CROs and COOs: Understand your **third-party relationships** and get regular updates on the risks posed by interacting with them and their connectivity to your organization.
COO: Update and rehearse **response plans** to include supply chain compromise scenarios.
CDO: Strengthen your **data trust processes**. Data is the target for most attacks on the supply chain. Data trust and good third-party risk management go hand in hand.

For the CIO and CISO: Build **defense in depth** to prevent, detect and block threats that might begin inside your network or have access from a third-party supplier.
Collaborate closely with your third parties and build approaches for **exchanging threat intelligence** to secure your collective digital ecosystem.

Discovery and Disclosure

Discovery and disclosure of 0-day vulnerabilities—software bugs newly discovered by researchers—rose in 2021. These 0-days can be exploited for cyber attacks before the developer has a chance to make a fix (or “patch).

In 2021, vulnerability researchers saw the rise of more ways—**both legitimate and criminal**—to earn financial reward for their exploit development work.

Aside from researchers, criminal exploit brokers and private espionage companies are important players in the exploitation of 0-days. These actors **aim to exploit these vulnerabilities before the software vendors can distribute patches** and advisories.

Discovery and Disclosure

Takeaways

For boards. Speed is important when responding to 0-day vulnerabilities. Ask your management how they are improving their processes to **shorten the time from discovery to remediation** of 0-day vulnerability. Ask how they decide on prioritization of mission-critical assets.

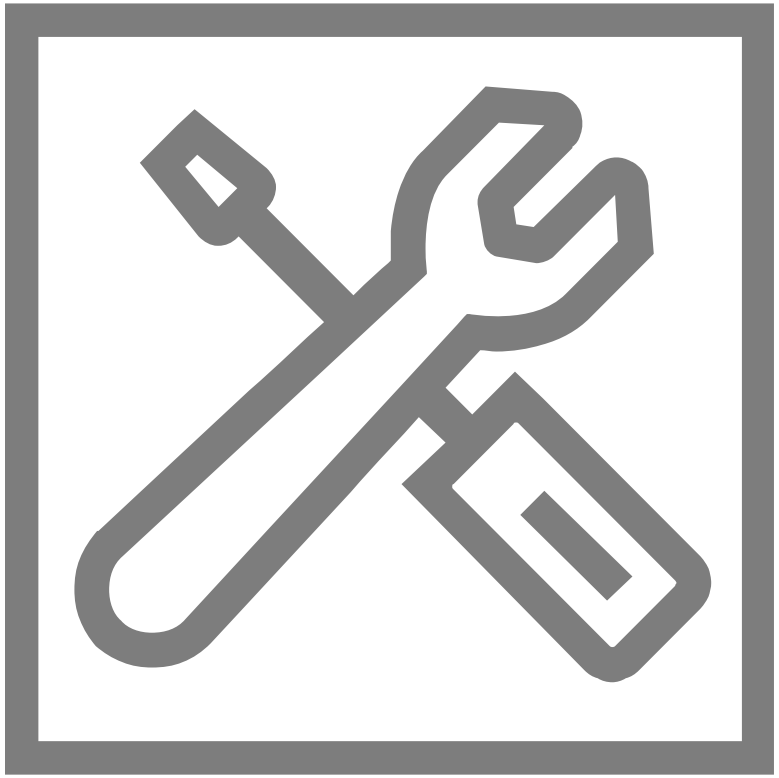
For the CRO and Business heads
Are you aware of your **mission-critical digital assets** and how you would you prioritize them for remediation?
Understand what would be needed to appropriately report the vulnerabilities that could make your digital products and services vulnerable to 0-day bugs.

For the CIO and CISO: The accuracy and quality of your asset inventory are critical. Improve your ability to quickly identify assets impacted by 0-day vulnerability through ongoing improvements to the **asset discovery and inventory** processes.
Shorten the time from discovery to remediation of 0-day vulnerability through ongoing focus on **automation and optimization** of the emergency patch management process.
Refine your **threat-hunting** capabilities to spot potential 0-days within your environment and define an approach for responsible disclosure

Cyber attack at scale

Cyber attacks at scale flared up in 2021 as quartermasters flourished.

Enter the commercial quartermasters: private companies that **sell offensive security** solutions such as spyware, 0-day exploits and related capabilities to entities. These are global operations: Customers of commercial quartermasters might be based in several, possibly mutually hostile, countries. Quartermasters **lower the barriers to entry**, since cybercriminals and nation-state actors **no longer need to develop their own malware**. Cybercriminals can **specialize instead in spreading malware** throughout the target's IT environment or deploying leased ransomware at scale across multiple targets. Commercial quartermasters drew attention in 2021 for zero-click spyware installed on smartphones of civilian targets.



Cyber attack at scale

Takeaways

For boards. Failure to adapt is failure. Ask your CISO about approaches they're taking to **keep pace with new and unknown threats** and how they can educate you.
Ask your CISO also about how they're **updating threat assessment continually**

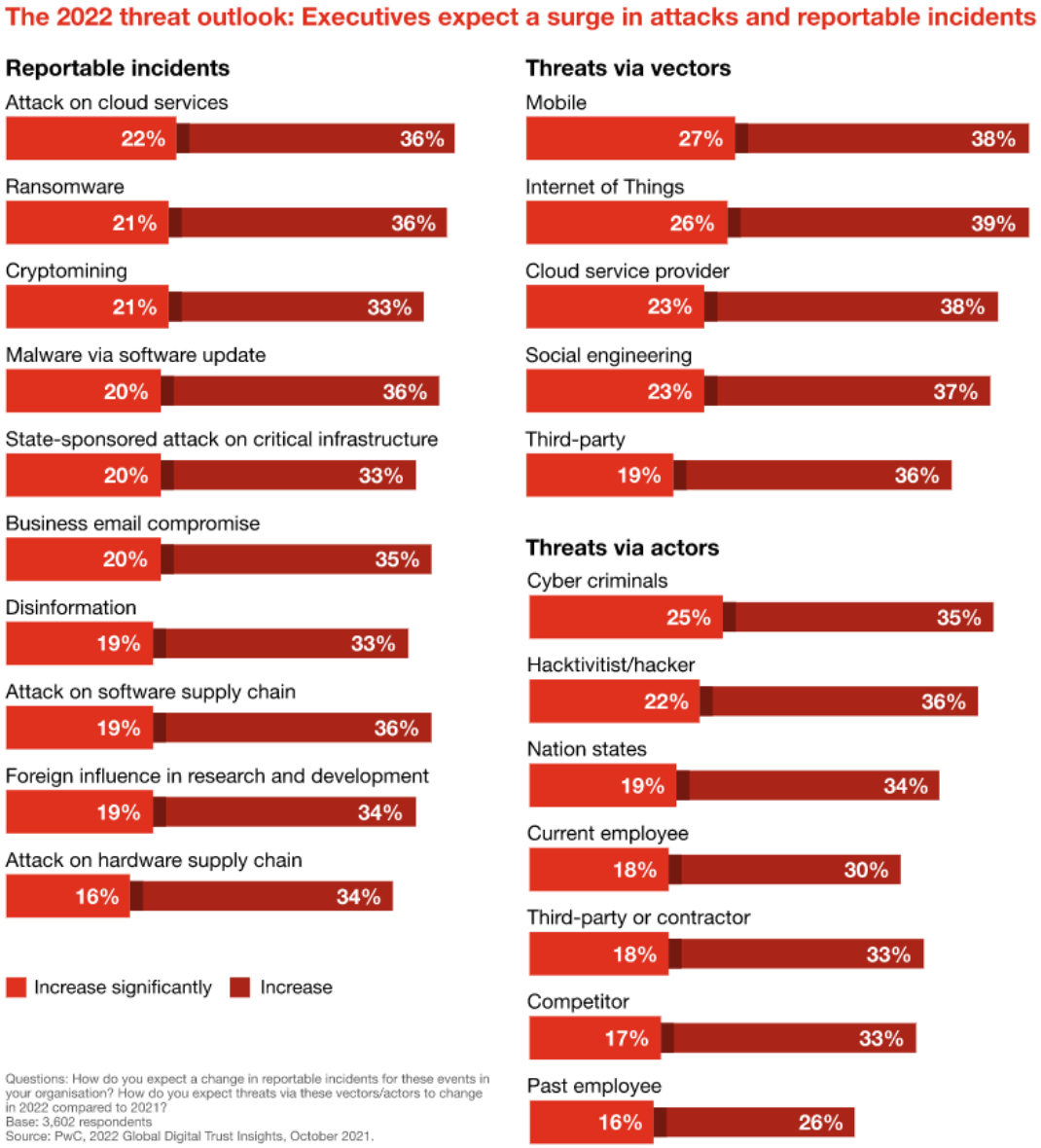
For the CRO and Business heads
Update your **enterprise cyber risk assessment** to account for the latest offensive security tools.
Determine if the changes in cyber risks will be sufficiently covered by your **cyber insurance**.

For the CIO and CISO:
Implement defense in depth. Organizations shouldn't rely on any one tool or security layer detecting or blocking 100% of all attacks. **Layered security** increases the probability that you will block or detect activity and gives you more information for responding to incidents.
To address the increasing scale of attacks, implement **intelligence- and automation-driven** approaches for detecting and responding to potential threats.

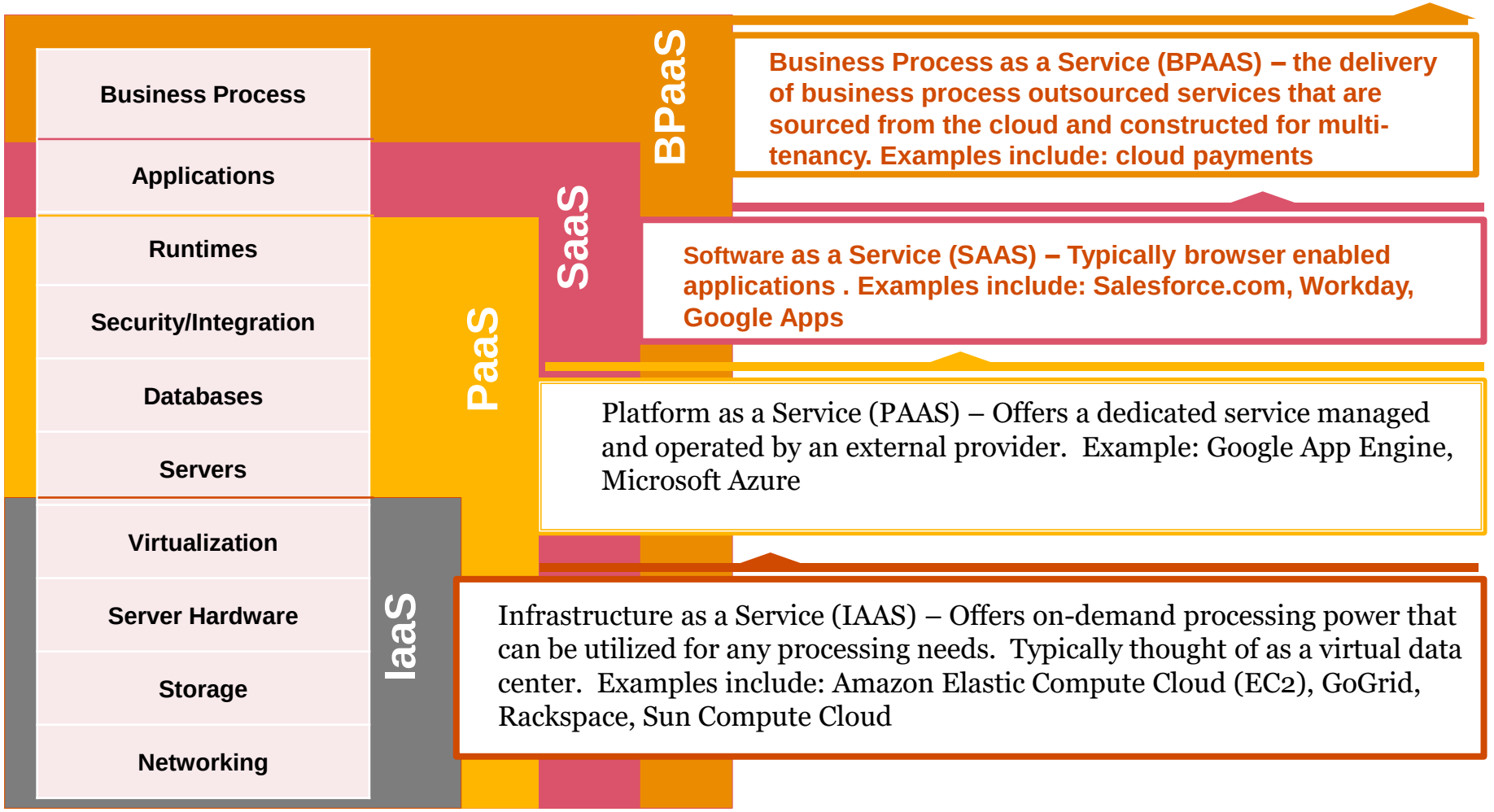
Looking to future: Cloud breaches are a top concern

More than half of 3,600 respondents to our 2022 Global Digital Trust Insights survey expect an **increase in reportable incidents**, with attacks on cloud services at the top of the list.

Attacks on cloud services are especially concerning as the pandemic has accelerated cloud adoption worldwide. For two years in a row, cloud security has been the top priority for cyber investments, according to more than 3,000 business executives who have responded to our annual surveys. And rightfully so. An overwhelming majority of cyber attacks in the past 18 months happened in the cloud, and nearly all could have been avoided had security been ready at the outset.



Looking to future: Cloud breaches are a top concern



Looking to future: Cloud breaches are a top concern

Takeaways

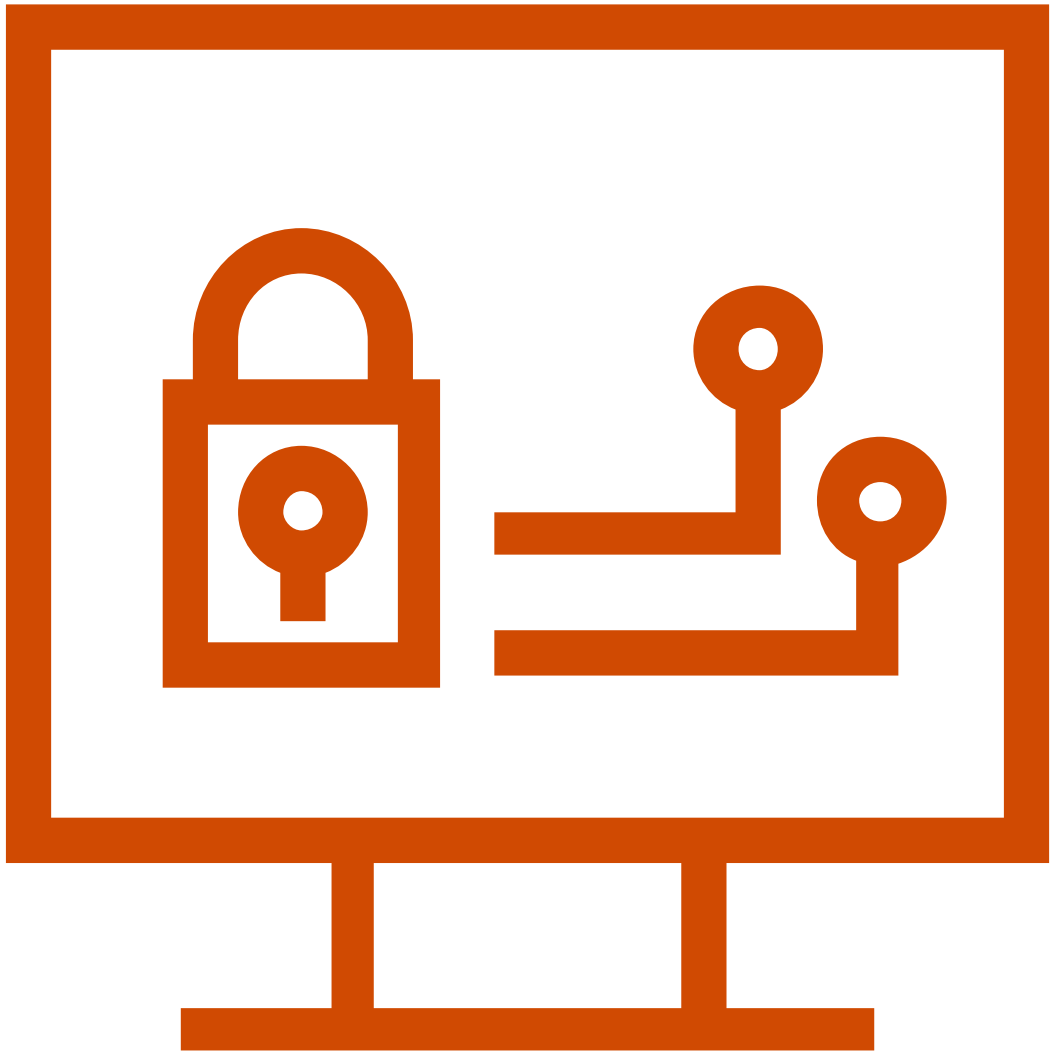
For boards. Traditional security approaches are not fit for multicloud environments.
Aside from oversight on the cloud strategy, ask management how they are **evolving the security framework for multicloud and hybrid cloud** environments. Conduct **crisis simulation**, from board level down to IT practitioners, to help prepare the entire organization and ensure everyone knows what to do if there is a cloud breach.

For the CRO and Business heads
CROs: Enhance the risk and controls framework to factor in the security challenges and opportunities presented by cloud.
Business heads: Understand how a cloud breach could impact your critical business services and mission-critical assets, and rehearse your **business continuity plans** for those scenarios.

For the CIO and CISO:
Put controls in place to **monitor new cloud functions** and make sure those updates don’t jeopardize your organization's security posture and/or regulatory obligations.
Embed security and privacy requirements into digital transformation programs and DevOps processes. Encode security policies and controls into the very fabric of your cloud environment. **Security-as-code** includes automation to keep the information and operations secure in your various environments, no matter what changes.

Summary

- Ransomware
- Supply chain compromise
- Discovery and Disclosure
- Cyber attack at scale
- Cloud Breach



Thank you

pwc.com