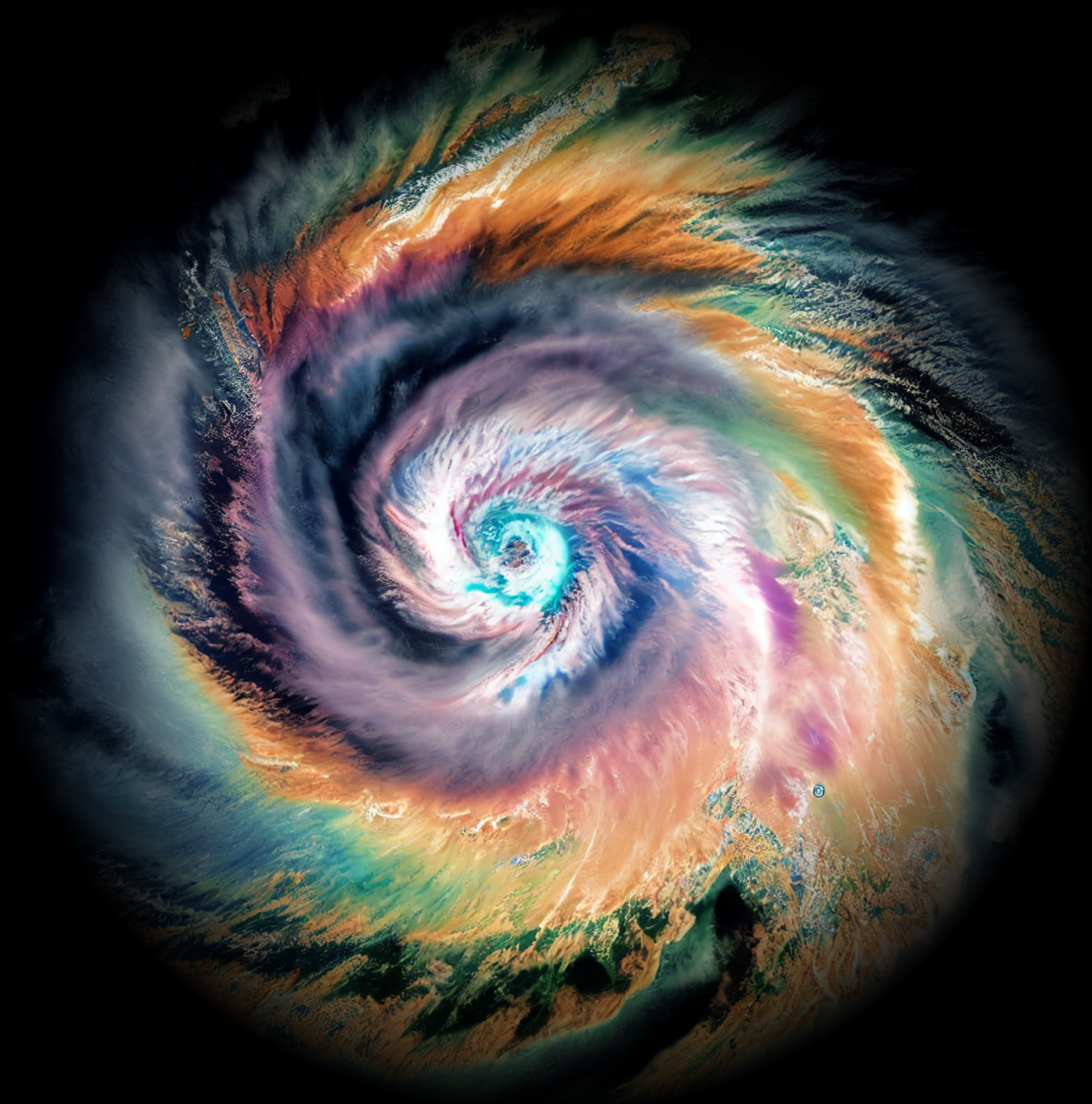
Deloitte.
Private



ERM and the fight to contain cybersecurity threats

Introduction

As organizations of all sizes and ownership types transact more business online, automate processes, and employ remote workers, the vectors for cyberattacks are expanding. In this environment, information assets such as email, company intellectual property, and client data can become valuable targets for hackers, cybercriminals, and espionage actors to exploit business users, employees, or other enterprise stakeholders. Though they may not have the high profiles their public counterparts do, privately owned enterprises are still at risk of cyberattacks. In some ways, private companies can be particularly attractive targets if their security practices aren't mature, potentially exposing their assets at great cost.

It's important for staff across the organization—especially within private enterprises whose cybersecurity teams may lack the resources to deploy an effective cybersecurity program—to learn how to protect systems and information from the growing list of information threats. The benefit of a strong detect-and-respond capability within an enterprise risk management (ERM) program is a lot like Doppler radar—working in the background conducting surveillance and tracking storms—allowing teams to detect and respond to cyberthreats as they arise.

A multi-front threat

Cybersecurity hackers are becoming increasingly sophisticated and productive, and organizations may not detect an attack until months after the fact. A 2023 survey shows that organizations took 204 days to identify a breach, and an average of 73 days to contain or resolve a breach once it was identified.

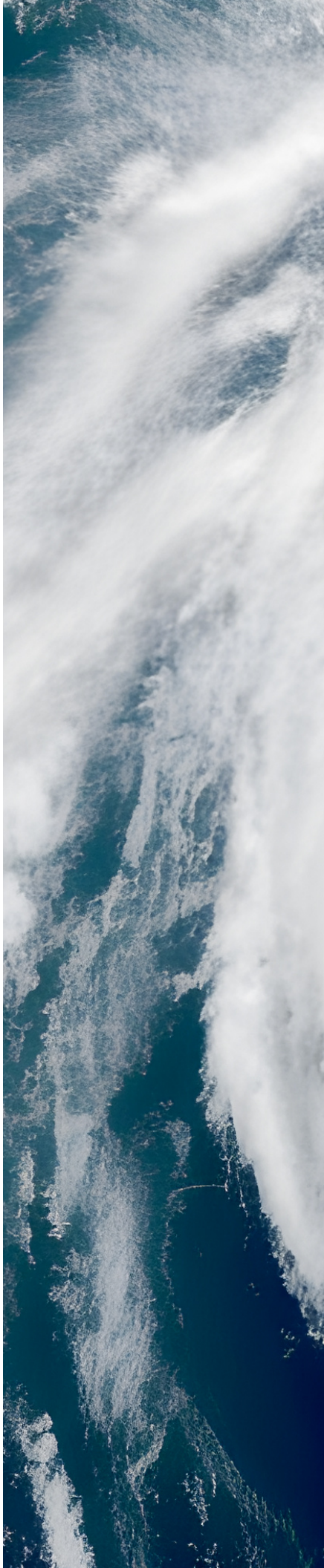
A common type of attack targeting private companies is ransomware, in which hackers extort organizations by holding information for ransom. In 2022, Deloitte observed more than 100 unique ransomware families, which share common codes and malicious commands. Predominant attacks include compromised credentials, external remote services and applications, and multifactor authentication fatigue. In the first six months of 2023, ransomware gangs extorted more than $449 million from victims, putting the attacks on track to approach the peak of nearly $940 million in 2021.

Our research also shows other types of attacks negatively impact companies, including social media impersonations of C-suite executives via fraudulent accounts, malicious social media accounts targeting C-suite executives, and phishing attacks that compromise business email accounts.

Third-party breaches and associate cyber risks are another area of concern. In a recent Deloitte study, we found that 74% of respondents have faced at least one third-party related incident in the last three years.

Patriotic "hacktivists" comprise another threat actor group who use information to shape geopolitical affairs using data leaks, ideological attacks, and website defacement. These attacks can sometimes be aimed broadly at belligerents and government regimes, but the effects trickle down to public services as well as private companies.

A common type of attack targeting private companies is ransomware, in which hackers extort organizations by holding information for ransom.



Assessing risk probability

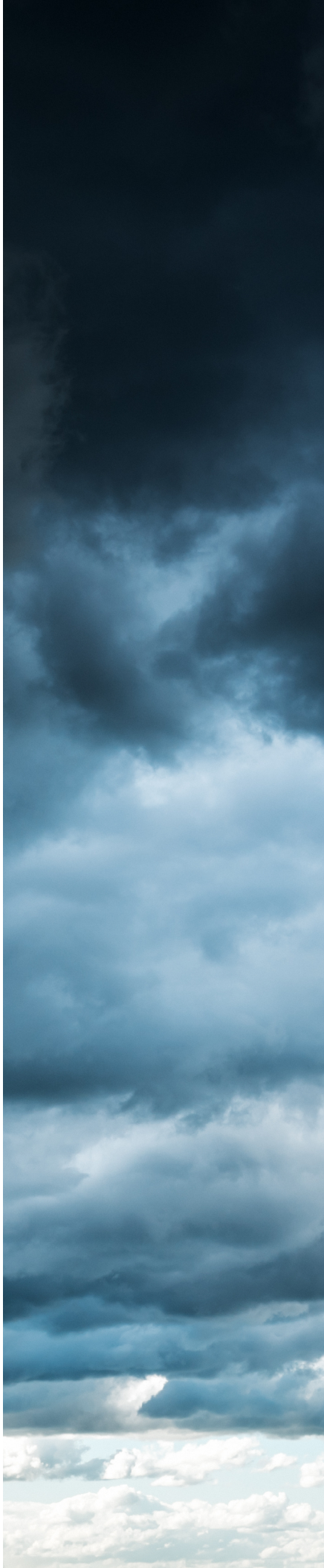
With the increase of cyberthreats, the stakes are rising, putting the onus on private companies and family enterprises to have effective detection systems. One leading practice private companies can consider is making a regular habit of developing a risk profile—assessing risk probability and the impact of threats. This involves determining the overall risk appetite for the enterprise in order to set the strategic tone for the overall enterprise.

Some fundamental identity and access management practices can be deployed to help avert a potential data security breach or loss. For instance, having an identity and access management system that includes things like privileged access management, governance, single sign-on, and multifactor authentication can be a solid approach. Additionally, constructing an enterprise architecture in which only certain individuals are granted access or privileges they need based on their role can limit potential paths to data and information breaches.

Another tangible step boards and CEOs can take is identifying a list of crown jewels—an organization's most critical assets. These prized assets might encompass customer data, transactional banking information, or valuable intellectual property such as formulas or patents. Determining what makes the list depends upon the industry, the organization's mission, and the nature of its operations. And it's not enough just to know what they are; organizations should know *where* they are and how they can best be protected.

Companies can also consider third-party providers for detection capabilities. But much like continuous radar scans of one's own organization, it's important to consider and monitor for threats within the third party's ecosystem. To that end, a leading practice is asking a set of questions of third-party risk management providers. That might include questions about the health of the supply chain, the location of vendors within the supply chain, and whether or not that third party has ever been breached.

Another tangible step boards and CEOs can take is identifying a list of crown jewels—an organization's most critical assets. These prized assets might encompass customer data, transactional banking information, or valuable intellectual property such as formulas or patents.



Spreading responsibility

Getting a handle on risks across an organization's ecosystem takes significant coordination—and the right risk management construct. For a smaller or less mature private company whose head of security is wearing multiple hats, this can add additional pressure to the job. The person may be head of IT security, but that means they're often also the IT director, in charge of privacy, and maybe hold another digital job altogether. There's often confusion on what the role of the head of security plays versus the executive team versus perhaps the board of directors.

Deloitte projects that cybercrime costs will escalate to $10.5 trillion by 2025—underscoring the need for robust security measures. Traditional breach detection times may lag for months, likely necessitating a more proactive approach to safeguarding data and systems.

The board is ultimately responsible for safeguarding the governance and viability of the organization. The question now is whether boards are able to get their hands on the right information to make risk-intelligent decisions.

Planning an incident response strategy

We've prepared a set of questions that leaders can pose to their organizations, regardless of where they are on the preparedness spectrum:

- Is cybersecurity enough of a priority for our organization that we have someone who's dedicated to the role and has the level of expertise to do the job?
- If and when we're breached, what is our incident response playbook, and have we effectively protected our crown jewels and key assets to avoid significant impact?
- If we suffer a ransomware attack, do we have proper backup and recovery systems in place? Can we operate resiliently through the attack and maintain essential business operations?
- Does our process for addressing third-party risk occur at the right frequency, and are we asking the right questions to determine the risk profile of our suppliers and third parties?

In our next installment in this series, we'll explore some common operational risks and how private companies can integrate operational risk management for more effective risk-taking.

NEXT UP IN OUR SERIES

Smart monitoring for operational risks
This article will explore common operational risks—such as supply chain, alliances, and third-party vendors. It will discuss the implications on the organization and share ways private companies and family enterprises can integrate operational risk management for more effective risk-taking and competitive advantages.

Visit deloitte.com to catch up on other articles in this series.

GET IN TOUCH

Kevan Flanigan
US Deloitte Private Leader, Risk & Financial Advisory
US Deloitte Private Leader, Private Equity
keflanigan@deloitte.com

Tiffany Kleemann
Cyber & Strategic Risk Managing Director
tkleemann@deloitte.com

Deloitte.