Deloitte.
Private

Family business cybersecurity, 2026

The family business insight series

Interactive navigation

This report has been designed to deliver an interactive experience, which is available when opened in Adobe Acrobat and the report is downloaded to your personal computer. If you do not have Adobe Acrobat, you can download it for free. Please note that without using Adobe Acrobat or downloading the report to your computer, some or all of the interactive features may not be available, limiting your access to the depth of data available.

[Click here to download Adobe Acrobat]

Contents

Foreword 3

Key takeaways 4

1 Experience of cyberattacks 5

Fortifying the future: A multi-billion-dollar business enhances cybersecurity and embraces digital technology to stay ahead 9

2 Cybersecurity strategies 11

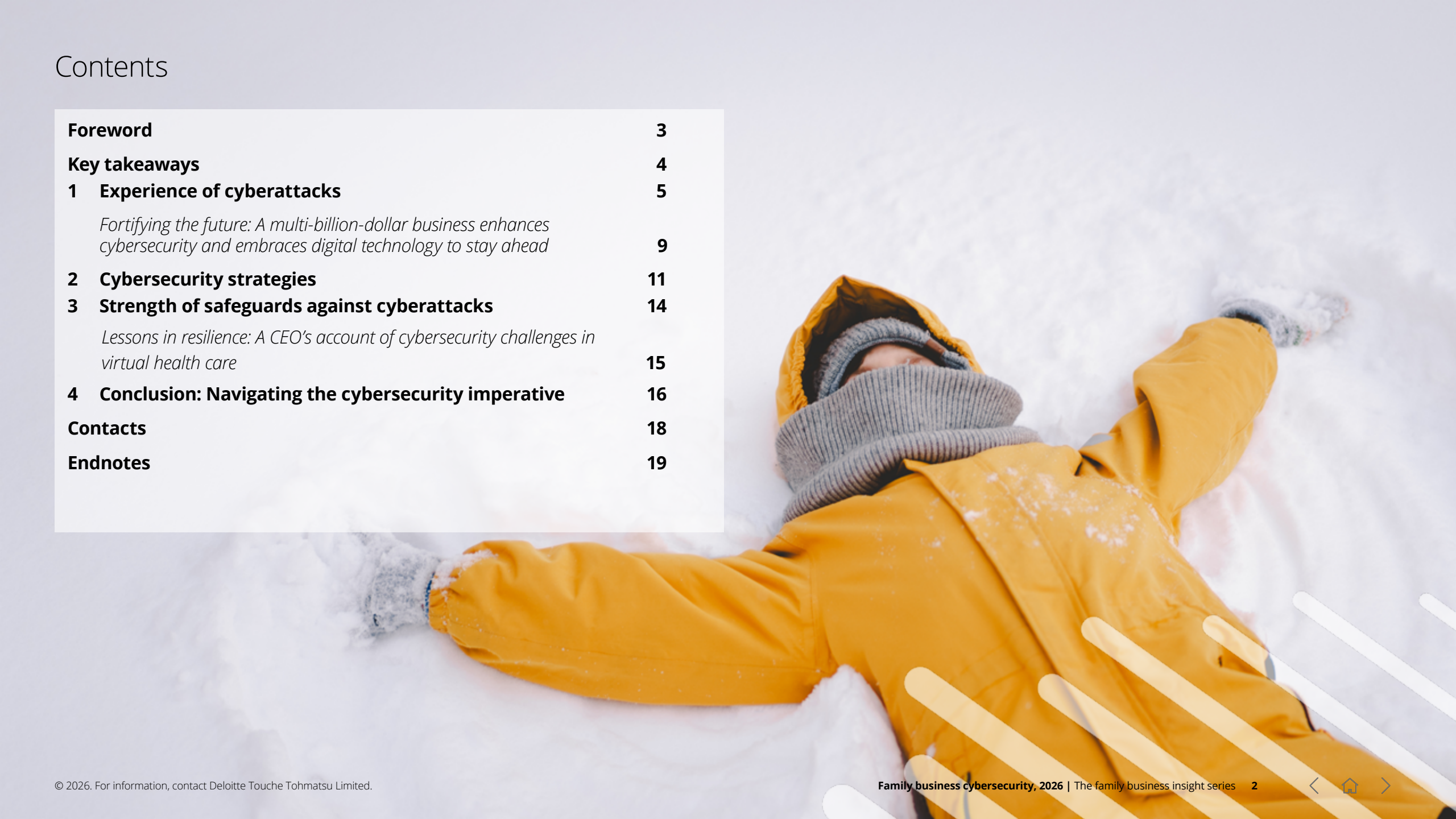
3 Strength of safeguards against cyberattacks 14

Lessons in resilience: A CEO's account of cybersecurity challenges in virtual health care 15

4 Conclusion: Navigating the cybersecurity imperative 16

Contacts 18

Endnotes 19



Foreword

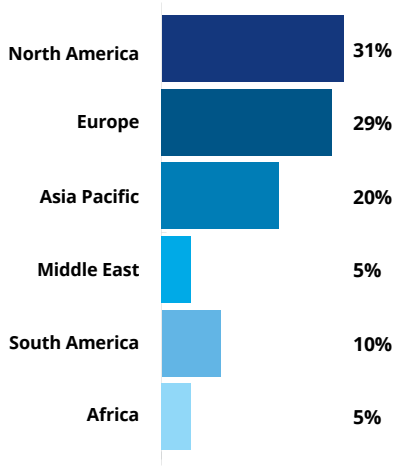
Welcome to the *Family business cybersecurity* report, part of Deloitte Private's *Family business insights series*. This series includes five reports that delve into: the evolution and character of the family business landscape globally; cybersecurity; technology transformation; succession planning and the next generation; and words of advice from leading family business executives.

This report examines family businesses' experience with cyberattacks, the means they are using to protect themselves, and what activities they can adopt to help themselves against future attacks.

To identify these insights, we surveyed senior executives from 1,587 family businesses worldwide between March and June 2025, with each having a minimum revenue of US$100 million and the families owning a controlling (51%+) share of the company. In 2024, these businesses generated an average revenue of US$2.8 billion and collective revenue of US$4.4 trillion. We also conducted in-depth interviews with 30 senior family business executives, many of whom are the heads of multi-billion-dollar families and 100+ year old family businesses. These interviews offer invaluable insights and advice that can help family businesses navigate the playing field and plan for long-term success.

We hope these insights prove useful in shaping cybersecurity planning for your family business, and we would like to offer a heartfelt thank you to the participants who generously shared their time and perspectives.

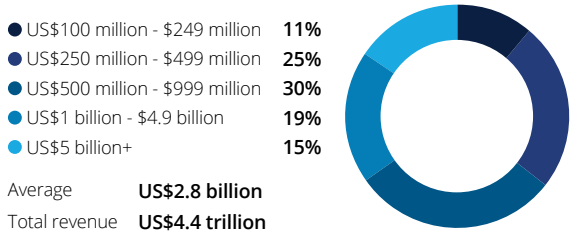
Participating family businesses' regional headquarters locations



Family businesses' 2024 (CY) annual revenue

Click on each button to view the data

Global | North America | Europe | Asia Pacific | Middle East | South America | Africa



Foreword
Key takeaways
1 Experience of cyberattacks
2 Cybersecurity strategies
3 Strength of safeguards against cyberattacks
4 Conclusion: Navigating the cybersecurity imperative
Contacts
Endnotes

Key takeaways

Cyberattacks are now widespread

Nearly three-quarters (74%) of family businesses globally have faced at least one cyberattack in the past two years, while a third (33%) have experienced two or more attacks. And exposure is near universal. While Asia Pacific leads in attack frequency, with 90% having experienced at least one attack, a substantial majority in each region has also experienced at least one attack—ranging from 61% in South America to 77% in North America.

Attacks are varied in nature

These attacks come in many forms, such as malware (experienced by 49% of respondents), phishing/business email compromise schemes (48%), social engineering (43%), third-party risk (40%), and insider threats (27%).

A need for more robust cybersecurity defenses

Despite the pervasiveness of these threats, merely 43% of family businesses globally report to have a “robust” cybersecurity strategy that has never failed them. A greater proportion (57%) has either a strategy with noticeable gaps (49%) or no strategy (8%). As a result, nearly half of family businesses (48%) feel only moderately prepared (39%) or not at all prepared (9%) should a cyberattack hit.

Basic defenses are widespread, but advanced measures lag

At present, most family businesses rely on basic first-line controls, such as software updates (59%), network security (57%), multi-factor authentication (MFA)/passwords (57%), and data backups (48%). However, reliance on advanced capabilities, such as incident response playbooks (40%), cyber maturity assessments (36%), vendor governance (32%), and identity management (31%), are less widespread. Reliance on basic cyber hygiene can help protect against opportunistic attacks, but more advanced measures are often better at protecting against sophisticated attacks.

Negative consequences have become commonplace

As a result of many family businesses having limited cyber defenses, it has become commonplace for them to experience loss or damage from an attack. In fact, most of those targeted have experienced financial (54%), operational (51%), and/or reputational (51%) harm. Only 4% of respondents globally say they have experienced no loss or damage, which is powerful evidence to suggest that more needs to be done to enable cyber resilience.

Foreword

Key takeaways

1 Experience of cyberattacks

2 Cybersecurity strategies

3 Strength of safeguards against cyberattacks

4 Conclusion: Navigating the cybersecurity imperative

Contacts

Endnotes

1 Experience of cyberattacks

Cyberthreats typically do not arrive with advanced notice. They ease in gently—through a convincing email, a vulnerable supplier, or an overlooked system update—and when they strike, the impact can feel personal, not just financial. For family businesses, a breach does more than disrupt business. It risks eroding reputations and family legacies carefully built over lifetimes.

This challenge spans regions and markets alike. From Singapore to San Diego and across the world, family businesses are grappling with the same digital vulnerabilities, even if the contexts differ. Some are pushing boldly into the future, adopting cloud services, digital payments, and AI-driven tools at a remarkable speed—sometimes faster than their safeguards can evolve. Others hold on to older systems that, while familiar, carry challenges of their own. What binds them together is a growing realization: Cybersecurity is not simply an exercise in preserving the status quo. It is a strategic choice that may define not only how competitive these businesses remain today, but also what kind of enterprise they hand down to the generations that follow.

Three in four family businesses have experienced a cyberattack

The survey data underscores both the pervasiveness and uneven distribution of cyberattacks against family businesses worldwide (figure 1.1). Globally, 74% of respondents report experiencing at least one cyberattack in the past 24 months, with Asia Pacific (APAC) based family businesses reporting the highest frequency (90% affected) and South America showing the lowest reported incidence (61% affected). This disparity reflects not only the different levels of exposure and digitalization across regions, but also variations in reporting, regulatory environments, and cyber resilience maturity.

Asia Pacific's elevated exposure may be explained by the region's accelerated digital adoption. North America's profile (77% attacked, reflects both high digital dependency and its attractiveness to adversaries.

By contrast, European family businesses report comparatively lower attack exposure (67%), with one-third of respondents indicating no cyber incidents. Europe's position could be linked to the General Data Protection Regulation (GDPR), which has prompted stricter controls on data handling, breach reporting, and cybersecurity standards across businesses.[1]

Foreword

Key takeaways

1 Experience of cyberattacks

Case study
Fortifying the future

2 Cybersecurity strategies

3 Strength of safeguards against cyberattacks

4 Conclusion: Navigating the cybersecurity imperative

Contacts

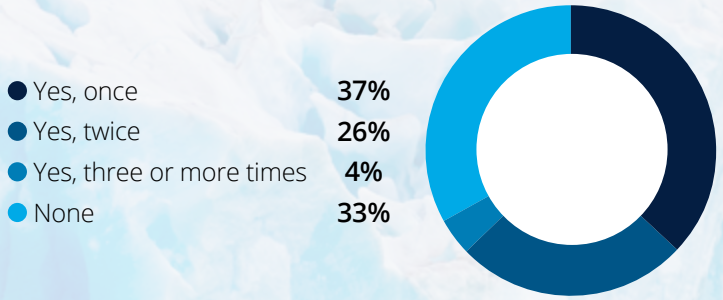
Endnotes

1 Experience of cyberattacks

Figure 1.1: Whether family businesses have experienced a cyberattack (successful or otherwise) within the last 24 months

Global | North America | Europe
Asia Pacific | **Middle East** | South America
Africa

Close



Types of cyberattacks:

- **Phishing and business email compromise (BEC)** – A widespread legitimate-looking email scam where a cybercriminal targets an employee to deceive them to transfer funds/release sensitive information/download malware. Smishing is phishing carried out by means of SMS (short message service) and vishing is phishing carried out by means of phone calls or voicemails.
- **Malware** – Malware is "a program that is inserted into a system, usually covertly, with the intention of compromising the confidentiality, integrity, or availability of the victim's data, applications or operating system, or otherwise annoying or disrupting the victim".[2] A common example of malware is ransomware (a type of malware that holds victims' IT systems hostage until monetary demands are met).
- **Social engineering** – Social engineering involves targeting an individual to take an unsafe action, such as transferring funds or releasing sensitive information. The most common forms of social engineering are phishing/BEC and pretexting (gaining a victim's trust and manipulating him/her into believing that the cybercriminal is someone they are not).
- **Third-party risk** – Where a third party (e.g., a supplier, contractor, or partner) with access to an organization's system or files damages or harms the business. This can be intentional (the result of a bad actor) or unintentional (the result of an attack on the third party that also impacts the organization).
- **Insider threat** – When an employee intentionally accesses confidential information. This might occur in the form of data manipulation, theft, leaking, and other threats.

Foreword
Key takeaways
1 Experience of cyberattacks
Case study
Fortifying the future
2 Cybersecurity strategies
3 Strength of safeguards against cyberattacks
4 Conclusion: Navigating the cybersecurity imperative
Contacts
Endnotes

1 Experience of cyberattacks

Malware and phishing most common types of cyberattacks

Family businesses worldwide are confronting a broad spectrum of attempted cyberattacks, from malware and phishing to insider threats and third-party vulnerabilities (figure 1.2).

Globally, nearly half (49%) report experiencing malware attempts, 48% phishing or business email compromise (BEC) schemes (i.e., widespread legitimate-looking email scams), and 43% social engineering efforts. These figures reflect an ever-growing threat landscape where cybercriminals increasingly take advantage of human and technical weaknesses in varied ways.

Regional highlights reveal notable disparities. Globally, 49% report malware attempts, leading the list. Certainly, malware is present in the digitally connected market of North America (54%) and, to a somewhat lesser extent, Europe (45%). But it is also pervasive in less digitally mature markets, with Africa at 56% and South America at 50%. INTERPOL's *Africa cyberthreat assessments report 2025* continues to list ransomware, banking trojans, and malware "as-a-service" among the continent's most prevalent threats amplified by rapid mobile/digital adoption and uneven incident response capacity.[3] In North America, high-value data and deep digital dependence make businesses attractive targets; *Verizon's 2025 Data breach investigations report* also shows system breaches dominated by ransomware and use of stolen credentials.[4]

Cyberthreats seldom occur in isolation. Research suggests that social engineering is often the pathway of more technical exploits such as ransomware. In that sense, insiders can unwittingly amplify many forms of threats. This challenge is exacerbated in truly global supplier ecosystems, given variations in reporting, regulatory environments, and cyber resilience maturity.

Examples of damage/loss as a result of a cyberattack

- **Financial** – Financial losses can arise on multiple fronts. For example, there can be direct losses from making payments to an attacker in the form of a ransom payment to recover access to one's system/files. These types of attacks can also lead to additional financial losses from operational downtime that directly impact a family business's ability to conduct business and serve the family. Additionally, when attacks are public knowledge, there can be a financial risk as a result of an impact to one's reputation and brand.
- **Operational** – A cyberattack may also result in operational disruptions through a loss of confidential data, a negative impact on employee morale (and subsequent retention rates), or a change in leadership at the office. For example, malware attacks may succeed in shutting down an organization's IT system, resulting in a halt to operations and possibly a loss of revenue.
- **Reputational** – Attacks could lead to reputational damage, such as negative media coverage, which could make third parties (such as potential lenders, investment managers, or other families) more reluctant to work with the affected families and family businesses.

Foreword

Key takeaways

1 Experience of cyberattacks

Case study
Fortifying the future

2 Cybersecurity strategies

3 Strength of safeguards against cyberattacks

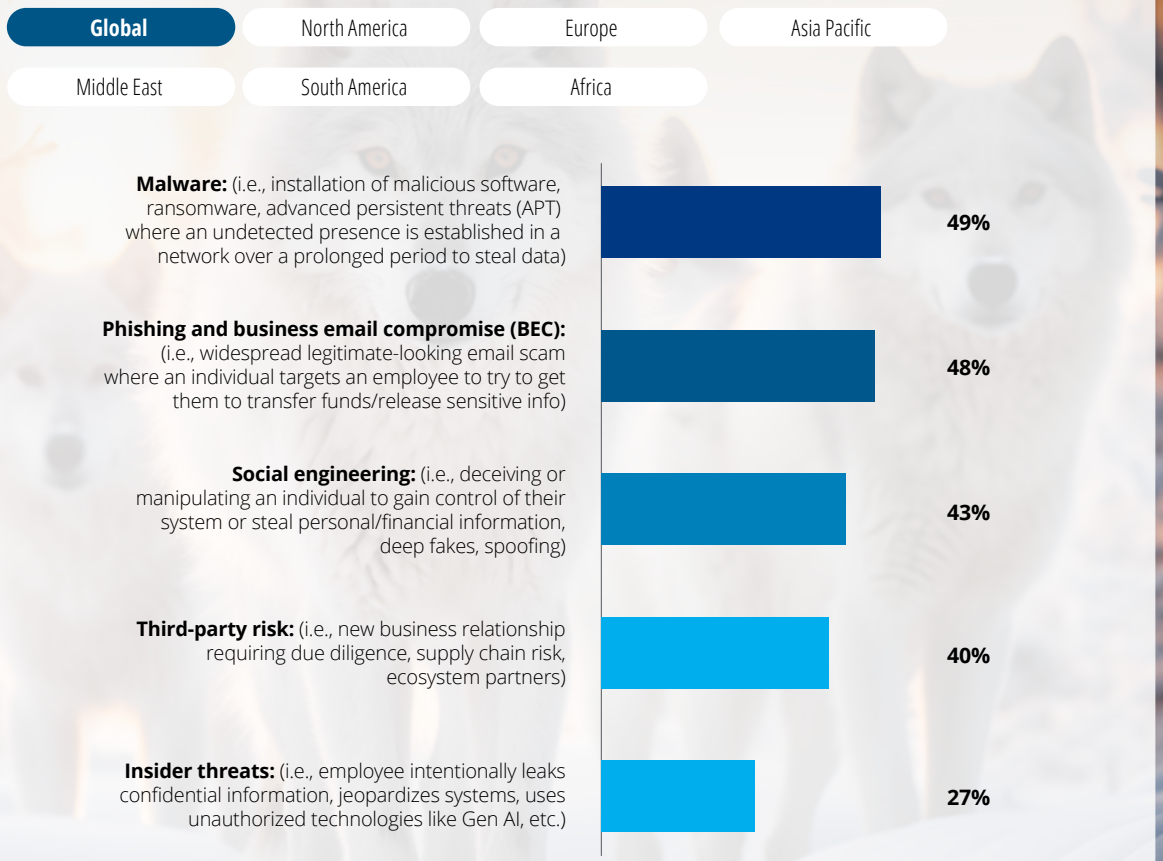
4 Conclusion: Navigating the cybersecurity imperative

Contacts

Endnotes

1 Experience of cyberattacks

Figure 1.2: The types of cyberattacks family businesses have experienced (Multiple options permitted)

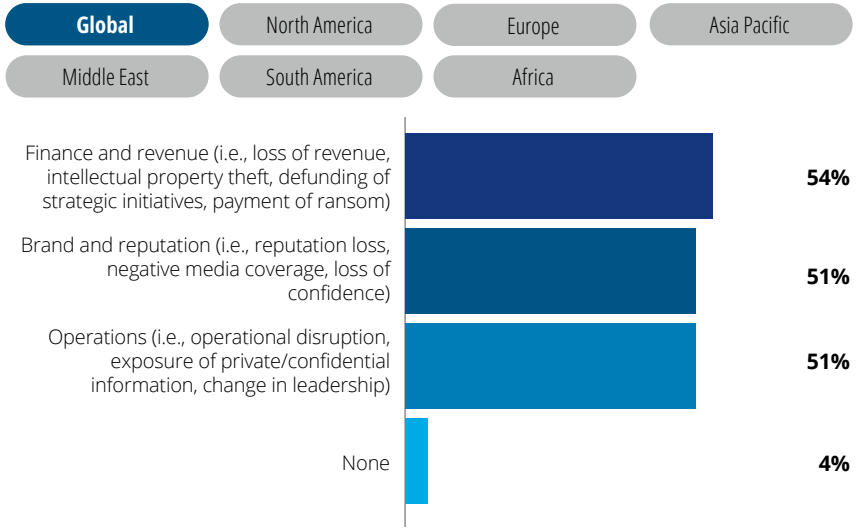


Modern cyberattacks are often scathing

At a global level, the impact of cyberattacks on family businesses is evenly distributed across financial, reputational, and operational domains at 54%, 51%, and 51% of respondents, respectively (figure 1.3). This underscores the multidimensional nature of cyber risk, where a single breach can simultaneously trigger monetary loss, reputational harm, and operational disruption. This makes sense as an attack such as ransomware/extortion can at once drain cash, halt operations, and spur reputational fallout. That relatively few respondents (4%) reported no harm from cyberattacks is consistent with the view that modern attacks are rarely consequence-free.

> *An employee was phished, allowing attackers to access our system for 45 days. They intercepted invoices and redirected payments, resulting in a loss of over US$500,000, which we never recovered. This incident underscored the importance of robust cybersecurity measures and vigilance across our organization.*
>
> **Family principal and CEO,** manufacturing company, United States

Figure 1.3: The negative consequences of the cyberattack(s) (Multiple options permitted)



Foreword
Key takeaways
1 Experience of cyberattacks
Case study
Fortifying the future
2 Cybersecurity strategies
3 Strength of safeguards against cyberattacks
4 Conclusion: Navigating the cybersecurity imperative
Contacts
Endnotes

Fortifying the future: A multi-billion-dollar business enhances cybersecurity and embraces digital technology to stay ahead

A leading US-based consumer products manufacturer shares how the family-owned business is strengthening its cyber defenses and adopting new digital tools to help them stay nimble and secure in today's evolving risk landscape.

In Deloitte Private's recent family business survey, respondents cited a lack of preparedness for cyberattacks as their top internal risk. How is your company addressing this challenge—and building resilience across the business?

We use third-party cybersecurity software but run it entirely in-house to maintain control and oversight. Recently, we adopted a system that uses AI agents to detect the most credible threats in real time. This is a major step forward from our previous approach, where people in our security operations center monitored systems and flagged suspicious activity, as they triggered many false alarms that drained staff's attention and sense of urgency. Now, when the alarm goes off, people know it matters.

While agentic AI plays a critical role in our cyber defense, the broader rise of AI is also fueling a new wave of cyberthreats. As more businesses adopt AI tools to generate insights and support decision-making, they often share vast amounts of sensitive data with AI startups, which operate in the cloud and have varying levels of security protocols that can create a new channel for potential attacks.

We are taking a more measured approach in our use of AI because of these vulnerabilities. There are no guarantees of security, and in many cases, even well-vetted companies offer little real protection. While others may rush in for fear of missing out on the AI revolution, we are taking a more deliberate path. We would rather be a fast follower than operate on the bleeding edge.

Foreword

Key takeaways

1 Experience of cyberattacks

Case study
Fortifying the future

2 Cybersecurity strategies

3 Strength of safeguards against cyberattacks

4 Conclusion: Navigating the cybersecurity imperative

Contacts

Endnotes

How are you preparing employees to recognize and respond to AI-driven cyberthreats?

AI poses a growing threat to businesses in ways that are harder to detect, especially as the technology becomes more accurate and sophisticated. For example, just a few years ago, phishing emails were often obviously fake with misspellings and poor grammar. But today, they are AI-generated and can easily trick employees into clicking on them. Malicious actors can also profile an employee's writing style and tone, generating emails that are highly convincing.

In addition to our cybersecurity software, we prioritize training and informing employees about the risks and how they play an important role in helping to prevent a cyberattack. We hold regular webcasts and live sessions with employees at all levels of our organization. In a recent webcast, our Chief Information Security Officer (CISO) opened with a deep-fake video of a senior finance executive. When it was revealed that it was not really him, people were shocked. That opened a lot of people's eyes to cyber deception and threats.

Our CISO emphasized the importance of communicating any potential breaches immediately—do not try to hide them. Every second counts to stem the threat, and we believe no employee should be reprimanded for making a mistake or getting tricked. This is an important message because it is human nature to think you might face negative repercussions for making a wrong decision, and this could lead to breaches not being reported.

Have you ever experienced a noticeable hit from a cyberattack?

The rigor of our tools and the vigilance of our people have helped protect us so far, but we know we are always vulnerable. Fortunately, the most significant issue we faced amounted to less than US$20,000. A small third-party vendor at one of our facilities had been attacked, and a hacker gained access to their system and monitored their activity for months. Because the owner regularly communicated with our accounts payable team, they were not suspicious when they received an email from her about a new bank account. In fact, because the hackers had infiltrated the owner's system, they were able to send the message directly from the owner's email account. Our team sent the payment as requested, unaware of the breach. The problem only surfaced when the owner followed up, asking about the missing payment. Unfortunately, the owner was unable to recover the payment, even after contacting the FBI. The hacker was untraceable.

After that incident, we instituted a strict validation policy: no payment or account changes are processed unless they are confirmed independently with a trusted contact in our system, not in an email chain. It is about checks and balances, a rigorous process to validate all requests as a first step.

Our family business report notes that the number one priority for companies this year is to build out their technology transformation platform. What are your efforts here?

We are launching a partnership with a leading software provider to implement their integrated tools platform, tapping into their AI-powered chatbot, analytics, and other advanced applications. This allows us to leapfrog in key areas while reinforcing trust in our security protocols.

We are also working to integrate our core operational systems—for example, feeding data from our time management application to our shop floor software, and tying that to our enterprise resource planning (ERP) and human capital platforms. Furthermore, we have begun using large language and data models to better understand the business. In addition to measuring productivity levels, we are looking to uncover best practices like how some teams maintain consistently low scrap rates. If we can identify and spotlight them and celebrate their success this can help other teams improve.

We cannot get those answers today because of disparate systems, but with these efforts, we are building the visibility we need to uncover deeper insights and take more informed action.

As we roll out these technologies, we are also redeploying our people into more strategic roles. With access to more integrated data, they are no longer just completing tasks, they are learning to make smarter decisions and think like business leaders. This evolution reflects our longstanding culture of agility, empowering our people to adapt, learn, and lead as our business transforms.

Foreword

Key takeaways

1 Experience of cyberattacks

Case study
Fortifying the future

2 Cybersecurity strategies

3 Strength of safeguards against cyberattacks

4 Conclusion: Navigating the cybersecurity imperative

Contacts

Endnotes

2 Cybersecurity strategies

Most family businesses fall short of cyber resilience

While 43% of respondents say that they have "a robust strategy that has never failed," a majority (57%) either have a cyber strategy that they acknowledge has gaps and "could be better" (49%) or no strategy (8%) (figure 2.1). While awareness of these gaps may be a first step and shows that family businesses recognize the importance of cybersecurity, these results also show that many, if not most, respondents fail to demonstrate full resilience or confidence in their strategies. Reconciling these gaps stands as a strategic imperative.

Figure 2.1: Whether family businesses have a cybersecurity strategy in place

Global | North America | Europe | Asia Pacific | Middle East | South America | Africa

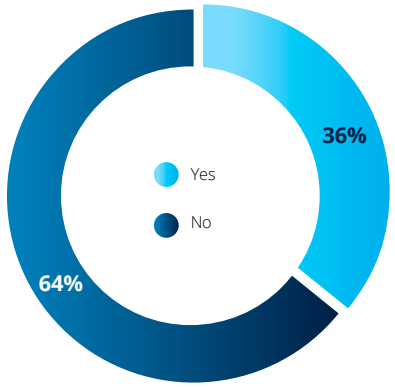
Tactical cybersecurity approaches favored by family businesses

In line with these sobering findings, just over one third of family businesses (36%) conduct cyber maturity assessments (to evaluate their ability to prevent, detect, and respond to cyberthreats against industry best standards), leaving the large majority (64%) which do not (figure 2.2). This points to the idea that family businesses often treat cybersecurity tactically (patching, antivirus, data backups) rather than through formal maturity programs or structured assessments such as those specified by the International Organization for Standardization, an independent standards development entity.[5]

> *Given the significant threat posed by cyberattacks, we have centralized cybersecurity at the holding company level, mandating standards and investments across all operating entities. This proactive, enterprise-wide approach ensures we detect and mitigate threats early—protecting our businesses and enabling us to sleep better at night.*
>
> **Partner,** major holding company, United States

Figure 2.2: Proportion of family businesses which conduct cyber maturity assessments

Global | North America | Europe | Asia Pacific | Middle East | South America | Africa



Foreword
Key takeaways
1 Experience of cyberattacks
2 Cybersecurity strategies
3 Strength of safeguards against cyberattacks
4 Conclusion: Navigating the cybersecurity imperative
Contacts
Endnotes

2 Cybersecurity strategies

Basic defenses are strong, while advanced measures lag

Most family businesses have implemented basic cyber hygiene, where the most fundamental practices have been broadly adopted (figure 2.3). Updated software (59%), network security (57%), MFA/passwords (57%), and data backups (48%) are the most common measures used globally. These are essential "first-line" defenses endorsed by major cyber hygiene frameworks.[6] At the same time, advanced capabilities such as cyber maturity assessments, vendor governance, threat intelligence, incident response playbooks, and identity management remain uneven and notably less widespread.

The gap between basic and advanced measures is also present across the regions. The North American and European regions show solid basic coverage and modestly higher adoption of advanced practices (e.g., incident response plan adoption being 46% in North America). Regulatory compliance requirements, such as GDPR, and historic breach costs drive investment in resilience, incident response, and vendor scrutiny.[7]APAC-based organizations are adopting basic measures, but lag on formal maturity assessments and vendor governance relative to exposure consistent with rapid digital transformation that outpaces governance.[8]

Overall, these gaps present a strategic challenge to family businesses. Basic measures may reduce many opportunistic attacks, but advanced controls—third-party risk management, identity governance, timely threat feeds, and practiced incident response—are often what limit damage from sophisticated attackers and supply-chain compromise, events that could result in substantial financial and operational repercussions, as well as erosion of brand trust.

> *Cybersecurity is a major focus for us, with dedicated teams and external partners continuously monitoring and testing our systems. The board regularly reviews our progress, and we have implemented comprehensive employee training and simulated phishing exercises to strengthen our defenses.*
>
> **CFO,** manufacturing company, Mexico

> *We maintain a risk committee and engage external consultants to assess cybersecurity, meeting stringent standards required for government and defense contracts, including two-factor authentication and Australian standard accreditation.*
>
> **MD and family member,** construction company, Australia

> *Cybersecurity is a constant, evolving challenge for any business today. While we have faced our share of phishing attempts and cyberthreats, our real defense comes from relentless employee training, robust insurance, and a commitment to learning from every incident.*
>
> **President and CEO,** retail company, United States

Foreword

Key takeaways

1 Experience of cyberattacks

2 Cybersecurity strategies

3 Strength of safeguards against cyberattacks

4 Conclusion: Navigating the cybersecurity imperative

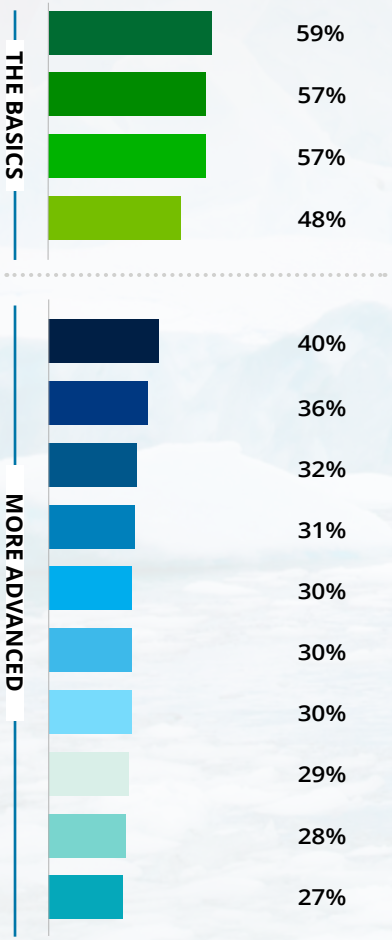
Contacts

Endnotes

2 Cybersecurity strategies

Figure 2.3: Cybersecurity measures that businesses currently pursue (Multiple options permitted)

Global | North America | Europe | Asia Pacific | Middle East | South America | Africa



- **Updated software including antivirus:** An inventory of computers, phones and other devices to support updated anti-virus/firewall software, software updates are installed as they become available, etc.
- **Basic network security including virtual private networks, secure email tools, etc.:** A virtual private network (VPN) is used to access the organization's network, and a connected device policy is maintained for the use of public Wi-Fi and home routers.
- **Strong password use and multifactor authentication:** Two or more pieces of information are required to access important websites, applications, etc.
- **Data back-ups: 3-2-1 rule:** 3 copies of your data are kept on 2 types of media, with 1 copy kept offsite.
- **Strong security policies including an incident response plan:** Policies and procedures related to day-to-day business operations security such as social media, payments, etc. and a defined approach to monitor and respond to potential threats that are actively implemented.
- **Cyber maturity assessment:** Assessments are conducted to evaluate the current state or level of cyber maturity and risk in the organization's environment from a people, process, and technology perspective.
- **Third-party management service providers:** Support managing and operating cybersecurity processes, controls, vendors, and operating models through shared responsibility.
- **Identity and access management capabilities in place:** Single sign-on, multi-factor authentication, privilege access management.
- **Insurance coverage:** Insurance which offers financial protection should the worst-case scenario materialize.
- **Key assets and crown jewels identification:** Identification of the key assets, intellectual property or trade secrets, sensitive customer information, and other critical information that is most important to the organization and should be protected.
- **A focus on talent-related risk and education:** Background checks are performed on employees and contractors, and staff are educated about cybersecurity risks, what to look out for, and how to prepare for a cyber incident.
- **Timely threat data:** You have an internal capability or have commissioned a service to monitor online open and closed sources to identify early warnings of potential threats.
- **A disaster recovery playbook:** An approach has been outlined for how the business would resume operations after a disruption caused by a cyberattack.
- **Know your vendors:** You review your vendors' own security posture, e.g., requesting security audit reports before contracts are signed.

Foreword
Key takeaways
1 Experience of cyberattacks
2 Cybersecurity strategies
3 Strength of safeguards against cyberattacks
4 Conclusion: Navigating the cybersecurity imperative
Contacts
Endnotes

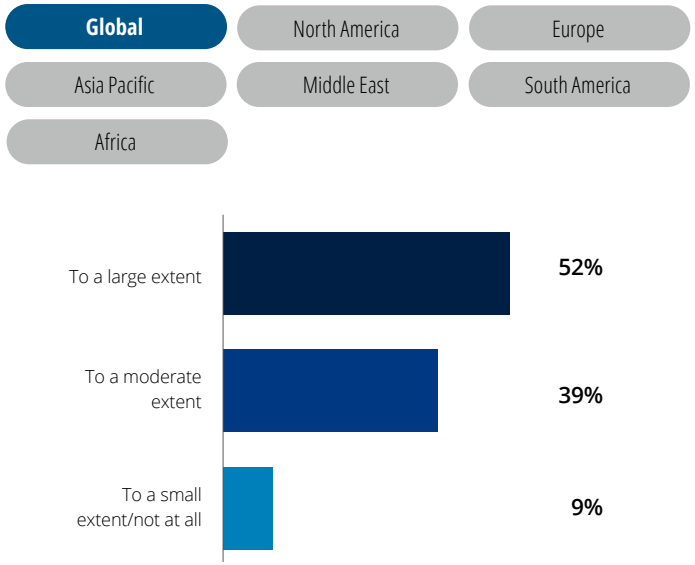
3 Strength of safeguards against cyberattacks

Overall, family businesses express relative preparedness, but deeper challenges remain

Globally, 52% of family businesses feel prepared "to a large extent" to safeguard their businesses against cyberattacks, but another 48% do not feel at all prepared or only feel prepared to a small or moderate extent (figure 3.1). This reflects a common trend: organizations feel partially prepared but recognize gaps in advanced readiness. Studies show—and the survey data confirms—that many businesses adopt basic controls but struggle with incident response, vendor risk, and advanced threat monitoring.[9]

Regionally, Asia Pacific leads with 58% feeling largely prepared. This is likely driven by digital acceleration and government initiatives like Singapore's Cybersecurity Act and Australia's Cyber Security Strategy. On the other hand, according to figure 1.1, some 90% of Asia Pacific respondents say that they have experienced at least one cyberattack within the previous 24 months, substantially ahead of the other regions, underscoring the gap that could exist between a *feeling* of preparedness and *actual* preparedness. Both North America and Europe show just above 50% who feel largely prepared. They are both mature cybersecurity markets with relatively strong regulatory frameworks (e.g., GDPR, Securities and Exchange Commission (SEC) cyber disclosure regulations, state privacy laws).

Figure 3.1: How adequately prepared family businesses feel to safeguard themselves from a cyberattack



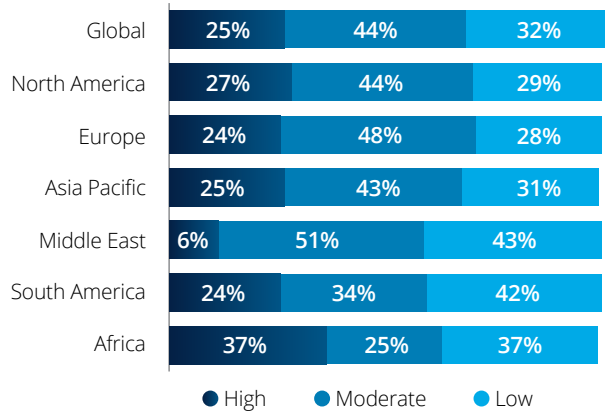
Most view cyberthreats as a moderate/high risk

Nearly 70% of respondents view cyberthreats as a moderate (44%) or high (25%) risk, while 32% view them as a low risk (figure 3.2). This spread suggests that, across the board, many businesses at least somewhat recognize the seriousness of cyber risks.

Both North American and European respondents see cyberthreats as a slightly greater risk than their regional peers. This may reflect the regions' mature digital transformation, exposure to sophisticated threats (e.g., ransomware, supply-chain attacks), and high-profile breaches that make cyber risk a board-level concern.[10] APAC-based organizations mirror the global threat sentiment. However, parts of the region—especially Southeast Asia—face rapidly increasing scam activity, including AI-powered phishing and deepfake frauds, that may not yet be fully appreciated by family businesses. Indeed, the United Nations Office on Drugs and Crime reports that the "spread of cyber-enabled fraud has since emerged as one of the most pressing law enforcement challenges facing the [Southeast Asian] region today."[11]

> *We have significantly strengthened our validation processes in response to increasingly sophisticated fraud involving the movement of funds. While we have not experienced any major financial losses, there have been a few instances where fraudulent instruments have resulted in minor losses. Given the volume of transactions and revenue flowing through the company, we are fully committed to preventing such incidents.*
>
> **Chairman,** construction, property services, and development group, United Kingdom

Figure 3.2: The degree to which family businesses view cyberthreats as a risk to their business over the next 12-24 months



Foreword
Key takeaways
1 Experience of cyberattacks
2 Cybersecurity strategies
3 Strength of safeguards against cyberattacks
Case study
Lessons in resilience
4 Conclusion: Navigating the cybersecurity imperative
Contacts
Endnotes

Lessons in resilience: A CEO's account of cybersecurity challenges in virtual health care

In this candid interview, a leader from a virtual medical care provider based in North America recounts the organization's experience navigating a significant cybersecurity breach. Through reflections on internal vulnerabilities, crisis response, and the impact on client trust, the interviewee shares practical insights on the real-world consequences of cyberthreats and the critical importance of robust security strategies and insurance support in health care technology.

How do you deem the current threat of cybersecurity to your business?

One of our portfolio companies, a virtual care provider offering remote patient monitoring, experienced a cybersecurity breach. It was one of the most difficult challenges we have faced. Trust is paramount in medical care delivery. A data breach erodes the confidence a provider has established with patients and the broader health care community and risks damaging the reputation of the entire organization. In our case, we could manage the financial damage and the operational issues resulting from the attack, but the reputational risk was the most important factor to control. We were able to preserve our credibility by receiving guidance from an outstanding team of legal, communications, and cyber experts assembled by our cybersecurity insurance provider. We were fully transparent with our customers from the start and maintained ongoing, open channels to address their concerns and restore confidence.

How did the breach happen?

As in many cyber incidents, the breach stemmed from human error: a programmer moved real patient data to an unsecured test site. Cybercriminals exploited that vulnerability and accessed 15,000 to 20,000 patients' data records.

What was the financial and reputational impact to your business?

The direct cost including legal fees, crisis communications, and new cybersecurity measures was just under US$2 million, nearly all covered by insurance. However, the reputational risk was far greater than the financial considerations. Over a six-month intensive response, we sustained our credibility by communicating openly with stakeholders—including hospitals, health authorities, and each affected patient through weekly updates and individual outreach. As a result, we lost only two customers, underscoring the effectiveness of prompt, transparent action and expert guidance.

What have you done to strengthen your cybersecurity?

After the breach, we added levels of protection throughout our systems, enhanced employee cybersecurity training, and built out a dedicated security team combining in-house staff with external partners. We now regularly conduct simulated attacks and frequent phishing exercises to keep our team ready for future threats.

What advice would you give other family business owners about cybersecurity protection?

Cybersecurity insurance is essential not only for coverage, but for immediate access to expert support. In our case, response teams were assembled within hours, saving us weeks of research, sourcing, and interviews. Just as crucial is a commitment to transparency, rapid stakeholder communication, and ongoing efforts to maintain strong internal controls and training. Those steps helped us protect both our reputation and our operations when it mattered most.

Foreword

Key takeaways

1 Experience of cyberattacks

2 Cybersecurity strategies

3 **Strength of safeguards against cyberattacks**

Case study Lessons in resilience

4 Conclusion: Navigating the cybersecurity imperative

Contacts

Endnotes

4 Conclusion: Navigating the cybersecurity imperative

The survey results paint a sharp image of the global cybersecurity landscape for family businesses—one marked by widespread exposure, regional disparities, and a persistent gap between basic and advanced cyber defenses. With nearly three quarters of respondents (74%) reporting at least one cyberattack in the past two years, it is clear that cyberthreats are neither rare nor isolated events. Rather, they pose a widespread threat that cuts across regions, sectors, and organizations of different sizes.

Family businesses are facing a barrage of cyberattacks. The data reveals that each region is at risk. The spectrum of threats is broad, from traditional attacks like malware and phishing to internal threats and supplier-related vulnerabilities, with attackers ever-evolving to seize advantage of human and technical frailties.

And the impact of cyberattacks is multidimensional. Financial, operational, and reputational harm often occur simultaneously, amplifying the stakes for family businesses. The survey confirms that cyber incidents are rarely consequence free; even a single breach can affect the entire organization.

While most family businesses have embraced basic cyber hygiene, such as software updates, network security, and backups, there remains a significant gap in the adoption of advanced capabilities. Cyber maturity assessments, vendor governance, threat intelligence, and incident response planning are far less common, leaving many organizations exposed to sophisticated attacks and supply chain compromises. This gap is evident across the regions.

The survey's findings converge on a clear strategic imperative: family businesses should consider moving beyond basic cyber hygiene to embrace an end-to-end, anticipatory approach to cybersecurity. This is not merely a technical challenge; it is a matter of the continuity of operations, the strength of the brand, and the durability of the business over time.

Foreword

Key takeaways

1 Experience of cyberattacks

2 Cybersecurity strategies

3 Strength of safeguards against cyberattacks

4 **Conclusion: Navigating the cybersecurity imperative**

Contacts

Endnotes

4 Conclusion: Navigating the cybersecurity imperative

Actionable recommendations: Building cyber resilience in family businesses

To address the challenges highlighted by the survey, family businesses may consider the following best practices:

1. Position cybersecurity as a business imperative

- Treat cyber risk as integral to overall enterprise risk, not just a technology concern.
- Involve the board and executive team in shaping strategy and ensuring that the right investments are made.
- Reinforce the message that protecting digital assets is a mutual responsibility across the organization.

2. Perform ongoing cyber maturity reviews

- Routinely benchmark against recognized standards to identify strengths and weaknesses.
- Make assessments a continuous cycle, updating practices as threats develop rather than conducting one-off or ad hoc reviews.

3. Fortify core and advanced protections

- Consistently implement baseline safeguards, from rapid patching and MFA, to segmented networks, and secure, tested backups.
- Strengthen resilience with advanced capabilities such as threat intelligence integration, access controls, third-party risk oversight, and incident response playbooks.

4. Build workforce awareness and manage insider risk

- Deliver focused training to help employees identify phishing attempts, manipulation tactics, and risky behaviors.
- Put in place monitoring tools and clear policies to detect and mitigate risks stemming from both accidental and intentional insider activity.

5. Develop and validate response and recovery procedures

- Establish well-defined response processes and test them through regular simulation exercises.
- Embed cyber incident management into wider business continuity and disaster recovery frameworks.

6. Tap into peer networks

- Collaborate with cybersecurity firms, professional networks, and other trusted allies to stay ahead of emerging threats.
- Take part in peer-to-peer forums to gain insight into sector-specific risks and shared defense practices.

7. Bolster vendor and supply chain resilience

- Assess the security posture of suppliers and contractors, integrating cybersecurity standards into procurement and contractual agreements.
- Maintain ongoing oversight of third-party risks, recognizing that supply chain compromise is an increasingly common attack vector.

8. Take charge of regulatory shifts

- Keep track of changing requirements and regulations, and maintain up-to-date compliance practices.
- Proactively invest in capabilities that position the organization to help satisfy future compliance demands.

Final thoughts: Turning awareness into impact

The survey results offer both caution and opportunity. Family businesses are increasingly conscious of the risks that confront them, yet many remain at a crossroads, caught between basic defenses and the need for advanced resilience. The path forward requires leadership, prudent investment, and a culture of unceasing improvement.

By embracing cybersecurity as a strategic business imperative, family businesses can not only defend against today's threats but also lay the groundwork for sustainable growth within an increasingly digital world. The time to act is now: closing the cyber resilience gap is not just about mitigating harm; it is about building trust, protecting legacy, and securing the future for generations to come.

Foreword
Key takeaways
1 Experience of cyberattacks
2 Cybersecurity strategies
3 Strength of safeguards against cyberattacks
4 Conclusion: Navigating the cybersecurity imperative
Contacts
Endnotes

Contacts

Luc Brucher
Partner | Government and Public Services Leader and Deloitte Private Leader
Direct: +352 45145 4704
lbrucher@deloitte.lu

Stéphane Hurtaud
Partner | Cyber Risk Leader
Direct: +352 45145 4434
shurtaud@deloitte.lu

Maurice Schubert
Partner | Advisory & Consulting
Direct: +352 27331 5256
mschubert@deloitte.lu

Maxime Verac
Partner | Cyber Risk
Direct: +352 45145 4258
mverac@deloitte.lu

Endnotes

1 Amoo, O. O., Atadoga, A., Osasona, F., Abrahams, T. O., Ayinla, B. S., & Farayola, O. A., GDPR's impact on cybersecurity: A review focusing on USA and European practices, p. 1338-1347, 2024

2 National Institute of Standards and Technology, Computer Security Resource Center Glossary.

3 INTERPOL, 23 June 2025

4 Verizon, *2025 Data breach investigations report*, p. 26

5 World Economic Forum, Here's how SMEs can turn cybersecurity risk into opportunity | World Economic Forum, 30 July 2024

6 Cybersecurity & Infrastructure Security Agency, *Cybersecurity best practices*

7 TechRadar Pro, *Compliance is evolving — Is your resilience ready?*, 2024

8 Aon, Asia-Pacific's commitment to cyber security pays off, 30 May 2025; CIO World Asia, *Cyber budgets surge as mid-market firms in APAC struggle with AI security gaps*, 30 May 2025.

9 World Economic Forum, 2024

10 Reuters, ESG Watch: Companies 'complacent about cybercrime,' despite rise in risk from AI, 3 February 2025.

11 United Nations Office on Drugs and Crime, *TOC convergence report 2024*. ROSEAP

Foreword

Key takeaways

1 Experience of cyberattacks

2 Cybersecurity strategies

3 Strength of safeguards against cyberattacks

4 Conclusion: Navigating the cybersecurity imperative

Contacts

Endnotes

Deloitte.
Private