
avanade
Do what matters
Banks and cybersecurity:
building resilience

It's getting tougher

Banks take on average 233 days to detect and contain a data breach. By comparison, it takes 72 minutes for a phishing attack to uncover private data. There are over 4,000 password attacks every second in 2023, an increase by a factor of eight compared to 2021.

According to the IMF, attacks on financial firms account for nearly one-fifth of the total, of which banks are the most exposed. The risk of extreme losses from cyber incidents is increasing. Indirect losses like reputational damage or security upgrades are substantially higher. The IMF reckon the financial services sector has suffered 20,000 cyberattacks in the last 20 years, causing $12 billion in losses.

One study showed that ransomware attacks on financial services have increased from 55% in 2022 to 64% in 2023, which is nearly double the number reported in 2021. In 2023, the average cost of a data breach in the financial services sector was $5.9 million (the average was $4.5 million). Banks could face fines up to 4% of global revenues under EU General Data Protection Regulation if confidential information becomes public. Recent shifts toward mobile platforms and remote work require high-speed access to ubiquitous, large data sets. This dependency makes the likelihood of a breach even greater.

And, with banks, there's always regulation. The Digital Operational Resilience Act (DORA) – effective January 2025 - will require banks to record all ICT-related incidents and significant cyber threats. DORA requires financial institutions under EU jurisdiction to follow rules of operational resilience for the protection, detection, containment, recovery and repair of technology systems under cyberattack. From October 2024, the EU's Network and Information Security (NIS2) directive will require banks to boost the security and resilience of critical systems and networks, with the prospect of severe penalties for non-compliance. It imposes stricter cybersecurity obligations on entities operating in critical infrastructure or important sectors, such as banking. As with all regulation, there's lots of it and it isn't always consistent across the various countries where a bank may operate.

More broadly, a study by the World Economic Forum with Accenture and BNY Mellon found that:

- Almost a third (29%) of businesses reported that they had been materially affected by a cyber incident in the past 12 months.
- 41% of those organizations that suffered a material incident in the past 12 months say it was caused by a third party.
- Fewer than one in 10 respondents believe that in the next two years generative AI will give the advantage to defenders over attackers.
- The advance of adversarial capabilities – phishing, malware development, deepfakes – was the biggest issue (46%).
- The number of businesses that maintain minimum viable cyber resilience is down by 30%.

More than twice as many small and medium-sized businesses compared to larger organizations say they lack the cyber resilience to meet their critical operational requirements. There is growing cyber inequity between organizations that are cyber-resilient and those that are not.

With an increasingly tough cybersecurity landscape, what are the key issues for banks?

The key threats

We have identified five areas:

The rise of cloud security. This year companies will spend $300 billion worldwide on cloud services. This inevitable move to the cloud has implications for security. Gartner estimates that in 2023 global sales of cloud security products grew by 32%, compared with 13% for computer security services overall. The need for data protection, specifically in a cloud context, is increasing.

Legacy is still a constraint. Banks have a legacy of security applications, often from acquisitive activity. For larger banks, Gartner estimates that they will typically have 50 to 70 security applications within their business, all working independently. Overlap and duplication are therefore common, with higher running costs and no clear understanding of which ones work and which do not.

Platforms versus best-of-breed. Cybersecurity platforms offer a one-stop-shop, simplifying management but impacting on functionality. However, demand for managed services, i.e., full-service offerings, is set to rise by as much as 10% annually over the next three years and cybersecurity providers are acquiring new businesses to improve their service portfolio. By way of comparison, best-of-breed solutions offer sophisticated tools but can struggle in areas such as user experience and data integration. Consequently, the lines are blurring, with platforms becoming more modular and integrating best-in-class security tools.

The growing skills shortfall. The WEF report acknowledges that although many employers are still looking to hire experienced cybersecurity professionals (33%), the number one way to fill these roles is by upskilling existing employees. 91% of organizations are willing to pay for cybersecurity training and certification for their employees. The highest barrier to cyber resilience is resources and skill gaps, followed by the cost of transforming legacy technology and processes. What is more alarming is that cyber talent is becoming scarcer. The shortfall is growing as regulators increase their monitoring of cybersecurity in banks. There are 4 million cybersecurity roles unfilled globally and the profession needs to almost double to be at full capacity.

The advance of AI. AI is already providing threat actors with additional capabilities in the areas of phishing, malware and deepfakes. Explaining outputs from the black box of large AI models is not easy. One of the most pressing AI concerns for banks is data security and privacy. As generative AI systems rely heavily on large datasets to function effectively, the potential for data breaches and leaks becomes a significant risk. There is also the need to meet regulatory compliance rules for generative AI, especially in high risk AI systems, such as the EU AI Act, for example.

Using generative AI to enhance cyber security

Banks are working out how generative AI can help them develop cyber resilience in order to combat the sheer scale and sophistication of attacks they are experiencing. As ever, generative AI is part of the solution – but also part of the problem. Although there's huge potential for AI in cybersecurity, banks struggle to trust autonomous, intelligent cyberdefense platforms and services. Attackers are increasingly looking to exploit AI applications with new attacks like prompt injections, wallet attacks, model theft, and data poisoning, while increasing susceptibility to known risks such as data breaches and denial of service.

Applying and using large language models (LLMs) in a security operations centre (SOC) is another way to adopt emerging technology into existing cybersecurity. LLMs can be used as a way of automating or assisting an analyst to identify threats with more accuracy. In fact, according to Splunk's The CISO Report, 27% of surveyed chief information security officers will use generative AI in their SOCs to do just that: provide data enrichment of alerts and incidents.

How can Microsoft help?

Microsoft has developed a Copilot for Security service. This is the first generative AI security assistant on the market. It simplifies the threat picture and can identify problems and automate responses, continually learning and improving to help ensure security teams are operating with the latest knowledge of attackers, their tactics, techniques, and procedures. During the chaos of multiple alerts, it offers a vulnerability summary, prioritizes risks based on the scale of the attack and gives recommendations – in minutes. It also provides an audit trail for investigations.

Copilot allows teams to share useful prompts, such as reverse engineering (how malicious code leads to breaches). Analyzing threats at machine speed provides early warning to detect malware, trojans and phishing that is vital to the success of any bank.

Its capabilities also offer solutions to the problem of disparate legacy systems and visibility gaps. By harnessing the built-in security capabilities of other Microsoft systems and taking data signals from software such as Microsoft Sentinel and Microsoft Defender Threat Intelligence, it can provide a holistic threat picture and offer suggested solutions.

This all directly helps overstretched teams, transforming how they operate and enabling them to quickly and accurately investigate and identify threats. In fact, early adopters found it enhanced productivity, especially among new security analysts, and achieved significant time savings of up to 40% on core security operations tasks.

Microsoft found that experienced security analysts using Copilot were **22% faster** at common security tasks, while also **increasing accuracy by 7%**. Most importantly, **97% said they wanted to use Copilot again** next time.

The benefits of Copilot:

Identify potential anti-money laundering issues, based on detecting high risk documents or people. Copilot is integrated into Microsoft 365 and automatically inherits all your company's valuable security, compliance, and privacy policies and processes. Your data never leaves its secure partition and is never used for training purposes.

Target fraud detection by analyzing policyholder data and identifying suspicious activity.

Leverage generative AI to swiftly distill complex security alerts into concise, actionable summaries, which then enable quicker response times and streamlined decision-making.

Receive actionable step-by-step guidance for incident response, including directions for triage, investigation, containment and remediation.

Microsoft already enables its clients to assess threats in other clouds they use - and has done so since 2022. It is an important capability, given that four-fifths of cloud users have data spread across several clouds, and one that some competitors do not have (witness Google's recent $23 billion bid for Wiz). As a market-leading cloud-native application protection platform, Microsoft Defender for Cloud helps businesses secure their hybrid and multi-cloud environments from code to cloud. Working with Microsoft, we are now releasing new security posture and threat protection capabilities to enable banks to protect their enterprise-built generative AI applications throughout the entire application lifecycle.

Bringing security to life

We've worked with banks around the globe to strengthen their cyber security posture, based on our knowledge of the Microsoft ecosystem. Here are some examples:

1

For a European bank

We extended security controls already in place for on-premises applications to their cloud applications. The client needed to control shadow IT, monitor well-known SaaS applications, protect the exposure of sensitive information and detect unusual behavior across cloud apps. Three main applications were integrated (M365, Salesforce and Azure) and every application had a dedicated set of alerts that allowed the team to trace anomalous behavior, from risky IP to confidential document sharing.

2

For an Asia-Pacific bank

We helped them achieve higher maturity levels for application control. Previous projects had failed due to the complexity of the environment. This included two test domains, one development domain, three production domains, 14 business units, 113 sub-business units, 50,000 workstations and 10,000 virtual machines. This meant faster responses to threats and quicker policy changes to reduce operational disruption. Cost savings came through lower staff numbers being needed to manage application control.

3

A North American bank

Wanted a proactive security control model with cloud-native capability. We improved their Azure governance posture, reduced compliance risks (in areas such as NIST and PCI DSS), developed a more robust multi-factor authentication process and provided a single source of truth for Azure identities throughout their lifecycle process.

4

A global bank

Lacked the ability to monitor cloud applications from a security perspective, despite cloud migration being at an advanced stage. This was due to complex integration issues and lack of internal capability. We designed the architecture and implemented it in six months, integrating four critical applications, and designing and implementing 100+ dedicated policies. This allowed the client to proactively and quickly monitor potential security incidents within its cloud application portfolio.

In our experience, we would suggest there are a number of key areas banks should focus on to develop cyber resilience.

Developing cyber resilience

Developing cyber resilience. Given the widening threat surface, you should regularly review your business environment, assess regulatory and compliance requirements, and ensure your security posture is robust and up-to-date.

Adopt a robust framework. The National Institute of Standards and Technology (NIST) framework is widely considered to be the gold standard. It categorizes cybersecurity capabilities across five core pillars: Identify, Protect, Detect, Respond and Recover. What's critical is that you spread your security solutions across all five pillars and don't put all your eggs in the Protect basket. We conduct NIST and generative AI risk assessments for a growing number of businesses. The Center for Internet Security has also published benchmarks for Microsoft products and services, including Microsoft Azure and Microsoft 365 Foundations Benchmarks.

Train your people. Your organisation is only ever as secure as its weakest link. With the sophistication of today's cybersecurity solutions, hackers are increasingly going straight to source and targeting employees to get them to unwillingly or unwittingly hand over their credentials. Training your employees on cyber awareness is therefore absolutely critical. Regular training that's relevant and engaging (we advocate gamification) or online forums where employees can share information will help reduce the likelihood of a breach caused by human error.

Maximize your existing assets to reduce investment. You probably have many of the licenses you need in your existing Microsoft enterprise agreement. Many of the security tools you use from Microsoft today, such as Microsoft 365 Defender and Microsoft Sentinel, already use machine learning and AI to help you detect and respond to attacks and risks in your environment. In some cases, they do so automatically, without requiring human interaction.

Identify key risks and threats. Assess the value of the data being used by generative AI on behalf of your bank and its users, such as risks to input and output data, PII, algorithms, models and human factors. You also need to secure your use of third-party systems, such as ChatGPT, for example, addressing prompts that can inadvertently expose users' confidential information.

Automate to speed up response times. Not only can automation help improve SOC operational efficiency, but it also reduces response times and means less reliance on skilled analysts to investigate and respond to common attacks, enabling them to focus on more sophisticated indicators of compromise.

Manage skill shortages. Copilot for Security uses Microsoft's generative AI Security Assistant to help detect threats, manage incidents, and improve your security posture. It can even help you address cyber-skills shortages. Avanade is one of only five Microsoft partners on the Design Advisory Council, helping to shape Copilot for Security and one of the first organizations to implement it internally.

Get started

Generative AI holds the potential to deliver tremendous business value because there are so many use cases in which it can speed and strengthen your operational security. This includes incident response, threat hunting, security reporting, compliance and fraud, security virtual agents and chatbot advisors, cybersecurity training, simulated attack automation and user behavior analysis.

A good place to start is our Microsoft Copilot for Security readiness assessment. We provide assessments in areas such as cloud security, zero trust and data privacy, as well as a security baseline workshop. We've also developed a NIS2 security accelerator which assesses current posture and vulnerabilities versus NIS2 goals plus a roadmap to remediation.

Contact us to find out more details.

Our banking expertise

What differentiates Avanade from competitors is our unique ability to harness the power of AI and help banks grow intelligently and resiliently. We're able to deliver on this promise thanks to our exclusive Microsoft partnership, our market-leading AI pedigree, the deep financial services expertise of our people, our modular approach and industry IP, and the breadth of our capabilities.

We work with 13 of the top 20 global banks and over 60% of the top 100. Microsoft Azure is trusted by 80% of the world's largest banks and 85% of GSIFIs.

Our unmatched Microsoft relationship means we gain privileged access to Microsoft's AI roadmap, including the evolution of pioneering solutions for banks such as Copilot and Fabric. We benefit from unique access and insights into Microsoft's solutions, ensuring we're able to unlock their full potential to address the needs of our financial services clients. For example, we've been working with our global client base to introduce Copilot for Microsoft 365 as part of Microsoft's Early Access Program – and applying the learnings into our work.

Visit **www.avanade.com/banking** for more details.

Why Avanade?

Because of the shift to remote working and the use of third parties, the move to cloud for scale and flexibility, and the associated rise of cyberfraud (especially deepfakes and ransomware), security has taken on a new level of importance. Avanade provides holistic security through advisory, security consulting and managed security services. We provide global delivery using proven methodologies and leading technologies. We deploy from the full portfolio of Microsoft security offerings and the broader Microsoft ecosystem and can integrate best-of-breed third-party solutions through partnerships with leading providers such as Quest, One Identity, Tanium and Zscaler.

We make a genuine human impact by helping clients protect the trust of everyone they serve.

2X winner
of the Microsoft Zero Trust Champion Award

2023 winner
in the External Identities category, Microsoft Entra Partner Excellence Award

#1
for Microsoft security certified personnel (Avanade/Accenture)

60,000+
Microsoft certifications – more than any other partner

We have advanced Microsoft specialisations in Identity and Access Management, information protection and governance, cloud security and Microsoft threat protection

Leader: IDC Marketscape
for Worldwide Cybersecurity Consulting Services 2024

Microsoft has named Avanade as a **Managed Extended Detection Response (MXDR) Partner.**

Member of the Microsoft Copilot for Security Design Advisory Council

Visit www.avanade.com/security to see how we can help you secure your bank.

avanade

Do what matters

About Avanade

Avanade is the world's leading expert on Microsoft. Trusted by over 5,000 clients worldwide, we deliver AI-driven solutions that unlock the full potential of people and technology, optimize operations, foster innovation and drive growth.

As Microsoft's Global SI Partner we combine global scale with local expertise in AI, cloud, data analytics, cybersecurity, and ERP to design solutions that prioritize people and drive meaningful impact.

We champion diversity, inclusion, and sustainability, ensuring our work benefits society and business.

Learn more at www.avanade.com