# Will today’s security stand up to tomorrow’s threats?

A holistic, long-term strategy is a key to business growth

# Executive summary

## Security isn’t just an IT concern any more. It’s a business concern for CxOs and their boards.

Avanade research[1] shows that 90% of C-suite executives lose sleep worrying about security breaches. And no wonder. Breaches can cost millions of dollars to address, tarnish a brand, keep companies out of new markets and cost CxOs their jobs.

With more threats coming from more sources, you can’t afford to just be reactive. You need a security strategy that uses holistic processes and the latest technologies to better defend against breaches and to detect and remediate the ones that still occur.

This point of view identifies the components of such a strategy, the value in building a business case for security spending and shows you how to get started.

90%

of global C-suite executives lose sleep worrying about security breaches.

[1] “Avanade Hot Topics Survey,” QuickRead Report, Wakefield Research, December 2017

# Which one are you?

## It's increasingly true that there are just two types of companies: Those that have been compromised by a cybersecurity breach, and those that will be compromised – but don't know when.

The point is: Every organization is vulnerable. Every organization should *act* as though it's vulnerable. That's not just good IT strategy – it's good business strategy, given that the average cost of a cybercrime incident climbed to $11.7 million per organization in 2017, up 23% from the previous year.[2]

And that's just the cost of detecting and managing incidents and containing the direct business disruptions they cause. There's more.

- **The long-term impact on a company's brand can be staggering.** Eighty-seven percent of consumers say they won't do business with a brand that's had a credit/debit card breach.[3]
- **A violation of the EU's General Data Protection Regulation** (GDPR) can cost a company up to €20 million ($25 million) or 4% of its total worldwide annual revenue. And GDPR is just the tip of the regulatory iceberg.
- **A security breach can hit a CEO where it hurts.** Such breaches, on sufficient scale, have cost CEOs their bonuses – or their positions.
- **The potential for litigation** underlies much of the concern about cybersecurity. This can come in the form of criminal or civil penalties and class-action suits for data breaches, or litigation around breach of fiduciary responsibility.

Case study

## *Energy retailer meets security needs with cloud solution*

A large energy retailer in Australia wanted a self-service platform to boost the customer experience while reducing costs. But it had to meet strict security requirements to maintain customer trust. Avanade helped it meet these goals with a Sitecore web content management solution hosted on Microsoft Azure Platform-as-a-Service.

[2] "2017 Cost of Cyber Crime Study," Accenture and Ponemon Institute

[3] "How does a data breach affect your business' reputation?" National Cybersecurity Institute, Feb. 16, 2016

# The threats will only grow

As more employees use more devices, the surface area that you must protect increases too. And then there's the cloud. How you implement your cloud environment affects how secure that environment will be.

The ranks of bad actors continue to grow too, including those with political or terrorist motives. Theft of intellectual property is also on the rise. And ransomware attacks against businesses have increased.

With more threats from more sources, your organization's risk may come as much from people as from any vulnerability in technology. That's because employees must always be on guard against security risks and continually trained to recognize new threats.

Case study

## *Global bank meets regulatory needs with Office 365/hybrid cloud*

This global top-20 bank leverages the Microsoft core platform and an Avanade-customized security stack to meet strict regulatory requirements. Its solution includes Microsoft Office 365 and a hybrid on-premises/Azure cloud environment to implement its privacy access model and satisfy more than 400 controls imposed by bank regulators.

# CxOs are insecure about security

Most CxOs have at least a general understanding of these threats – and it keeps them up at night. Ninety percent of global C-suite executives say they lose sleep wondering if their companies will experience the next big breach, according to Avanade research. And 53% say that new technology tools are barely keeping up with new threats.[4]

Executives are doing more than express concern; they're taking action. In 2017, UK executives told Avanade that IT security was their top strategic priority over the coming 18 months.[5] And Gartner has projected that worldwide spending on IT security products and services will reach $93 billion in 2018, up from $86.4 billion in 2017.[6]

Spending is up in part because CxOs, not just IT decision-makers, understand the risks – particularly the business risks – of security lapses. So do their boards. Security discussions and decision-making that once took place only within the IT department now take place in the C-suite and the boardroom. That trend will continue. Gartner, for example, projects that IT executives at all large enterprises will report to their boards on cybersecurity on a regular basis within two years.[7]

That's great as far as it goes. But will those reports and discussions drive your business to the rigorous security strategy it needs? To get to "yes," you need to envision the right security goals – and the right approaches to achieve them.

53%

of global executives say new technology tools are barely keeping up with new security threats.

[4] "Avanade Hot Topics Survey," QuickRead Report, Wakefield Research, December 2017

[5] "Putting the IT in Brexit," Avanade, 2017

[6] "Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017," Aug. 16, 2017

[7] "The 15-Minute, 7-Slide Security Presentation for Your Board of Directors," Gartner, May 29, 2017

# Start by envisioning strategic goals

## Much of security planning is about mitigating risks, and rightly so.

But as significant as those risks are, the goals of a security strategy should go further – because the potential benefits of comprehensive, effective security go further. Security should underpin the broader enterprise strategy. For example, Avanade has helped major businesses to implement their customer experience and digital workplace strategies with approaches that also advanced the security agenda. Here are some objectives to consider:

Security that complements and contributes to business goals. Don't think of security just as something that plugs the holes in your infrastructure. Think of it as a strategic asset to help power your overall business plan. Looking to move into new geographic markets? Expanding security and compliance processes to cover those markets will be crucial. For example, Siemens implemented a secure workplace solution to accelerate the pace of onboarding acquired companies and their employees, while maintaining security.

Security that enhances the brand. Earlier we cited the negative impact of security breaches on brand value. The opposite is also true. Consumers prefer brands that protect their data. Implementing security as a competitive advantage can increase digital trust in the marketplace, leading to greater brand value, revenues and market share.

Security that helps meet regulatory requirements. GDPR is the latest big change to the privacy and security regulatory landscape – but it's hardly the only governmental standard that businesses must meet. For example, Canada is considering new rules to protect personal information online.[8] And in the U.S., a number of states have introduced stricter privacy laws.[9] Beyond fines for noncompliance, companies risk precious time and resources defending themselves against alleged violations. Meanwhile, meeting privacy and security regulations can help companies gain access to crucial new markets, fueling growth in customers and revenues.

Security that's tailored to your specific needs. One-size-fits-all approaches seldom fit anyone, and that's true with security. Healthcare providers need to protect personal identities and both structured and unstructured data related to them. Other organizations may need to protect different high-value information assets – such as algorithms and design data. Some businesses have a broad web presence, others have a high proportion of mobile and remote users. You must understand your organization's specific assets and vulnerabilities, then adopt technologies and processes specially intended to address them.

[8] "Canada's Privacy Commissioner contemplates new online erasure, data protection rules," Reuters, March 1, 2018

[9] "GDPR isn't the only game in town: US state developments also looming," IAPP, May 17, 2018

# Making the business case for security

Many companies invest in security even without a business case. It's just something they know they must do.

But how much security they buy and which security technologies and protocols they choose can be influenced by a compelling business case. Elements of that business case can range from cost savings and avoidance to supporting new ways of working that speed time-to-market, increase sales and facilitate business expansion.

If you don't already have a business case for security, we recommend you build one. Here are factors you might want to include:

Cost avoidance. Because the costs of managing a breach and its aftermath can be so high – including internal costs, litigation, regulatory penalties, and impact on brand value and revenues – you can estimate the annual value of cost avoidance based on your security history or the experiences of similarly situated organizations.

Cost savings. There's plenty of competition in the market for IT security products and services. That gives you the opportunity to upgrade your security solution to both reduce costs and increase protection. A comprehensive suite solution can cost less than buying comparable standalone functionality – and work more reliably and seamlessly. This approach can deliver better protection and reduce the ongoing costs of licensing, maintenance, redundancy and portfolio creep. And it still allows for adding specific solutions from multiple providers if you choose.

Greater productivity and collaboration. Extending IT security to mobile and remote devices can give users secure access to core business applications and other IT assets from anywhere at any time. That can speed business processes that otherwise wait for workers to return to a central office. Those accelerated processes, in turn, can spur opportunity cost savings, increased revenues or both. New ways to push out secure infrastructure to remote locations can speed geographic expansion and make that expansion cost effective.

Case study

## *Siemens supports M&A with workplace security solution*

The industrial giant has some 350,000 employees, and thousands more can become part of the company in any given week as the result of merger and acquisition activity. Siemens gets those employees onboarded quickly, successfully and securely thanks to a migration factory solution built by Avanade that supports up to 25,000 user migrations each week.

# Recommendations for a holistic strategy

Given the increase in the numbers and types of security threats, you need a holistic, long-term strategy to address them. Here are some places to start:

Integrate for faster detection and response. Security strategies often are strictly reactive or just focus on preventing breaches. But they need to do both. The typical attack goes undetected for about 140 days.[10] That has to change. An integrated suite of products for IT security, rather than standalone offerings, can reveal holistic attacks that otherwise go undetected as security staff sifts through product-specific reports. Frequent automated compromise assessments, also called integrated threat hunting, are an important tool.[11]

Focus on your people. Executives are evenly divided on whether people or technologies represent their greatest vulnerability to breaches.[12] We believe people represent the greater weak point, in part because they must be educated continually regarding new attack vectors, such as ever-evolving phishing scams, and in part because a single slip-up in security process can moot the effectiveness of technological defenses.

While all employees need security training, this is another area where one size doesn't fit all. Your highest-risk employees – frequent travelers who use hotel and airport public networks, for example – need extensive training. So do C-level executives, who handle the most valuable IP of a company. As Forrester notes, training should focus on changing behavior, not just on raising awareness.[13]

Perfect your processes. How your people go about their work and how your IT assets use automated processes are as important as which technologies you deploy to deter and detect breaches. A governance, risk and compliance (GRC) framework helps to ensure your company achieves its business goals through a coordinated emphasis on proper governance, risk mitigation and regulatory compliance. If you don't already have such a framework in place, now is the time to establish it. GRC can boost performance and effectiveness throughout the business; tying your security strategy to GRC can help to make security an integrated part of everything your company does.

Don't forget the data. As you assemble the technology components of your IT security strategy, it can be difficult to know where to start. Identity access, devices, the cloud – all have to be provided to your employees and others in secure ways. But don't take your eye off the need for data security. Protecting your data in transit, wherever it flows, is as important as addressing data at rest on devices and platforms.

[10] "6 ways to launch a targeted cyberattack," CSO, Jan. 30, 2017

[11] In September 2017 Accenture, Avanade and Microsoft announced an alliance to create cyberdefense offerings that deliver faster, fuller response to breaches. The alliance is focused on managed security operations, incident response support and integrated threat hunting.

[12] "Avanade Hot Topics Survey," QuickRead Report, Wakefield Research, December 2017

[13] "Harden Your Human Firewall," Forrester, Feb. 2, 2018

# Avanade and Microsoft: The right security combination

Microsoft invests more than $1 billion annually on its security offerings. Consolidating your security spend on Microsoft may be the right investment for you. The company offers integrated, end-to-end security technologies that protect your data, devices, platforms, identity access and business apps, and that detect and analyze threats for faster remediation.

Microsoft 365, which combines Office 365, Windows 10 and Enterprise Mobility + Security, provides capabilities including: advanced attacks protection and remediation, mobile device and app management, identity and access management, cloud and SaaS app security, threat and malware protection, and more.

## The services to secure your business

But technologies alone won't secure your business. How you devise strategies and tactics to address your key challenges is another crucial part of security success. Whether your needs are best met by a pure Microsoft solution or by going beyond an integrated Microsoft platform, these technologies can be the core of your solution.

Avanade can help you on your journey – from defining your strategy, to implementing and managing a secure and integrated platform. Our deep expertise and security services pull it all together. We bring real-world experience to help you discover and think about gaps you may not know you have. Our services include:

- Identity and Access Management
- Workplace Security
- Cloud Security

Case study

## *Energy provider spurs transformation, meets EU regs*

A major European energy provider needed to meet EU requirements while spurring digital transformation with cloud-based collaboration. Avanade delivered with a solution based on Microsoft Office 365 and Identity and Access Management.

# Ready to make your business more secure?

Learn more about taking the next steps toward a holistic security strategy: www.avanade.com/security

North America
Seattle
Phone +1 206 239 5600
America@avanade.com

South America
Sao Paulo
AvanadeBrasil@avanade.com

Asia-Pacific
Australia
Phone +61 2 9005 5900
AsiaPac@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

Avanade is the leading provider of innovative digital and cloud-enabling services, business solutions and design-led experiences, delivered through the power of people and the Microsoft ecosystem. Majority owned by Accenture, Avanade was founded in 2000 by Accenture LLP and Microsoft Corporation and has 30,000 professionals in 24 countries. Visit us at www.avanade.com.

avanade