CISO Guide: 5 Imperatives to up your security game

avanade

Contents

Why CISOs need this guide

Today, enterprise security experts face a daunting, yet exciting new reality. The frequency and sophistication of cyber-security threats are at an all-time high. Yet, despite these challenges, security professionals have an extraordinary opportunity. Not only can a modernized security approach bring peace of mind and prevent loss, it can be used as a core driver of business outcomes, sustainability and transformation.

The fact is, modern security needs cannot be met by new technologies alone. In fact, 48% of executives say security threats are evolving faster than security technologies, according to Avanade's 2019 Hot Topics Survey. To close the gap, CISOs have discovered they need to evolve their ideas and adopt a set of new rules to ensure success.

This guide reveals five new imperatives for the CISO. From transforming the workplace, to optimizing operations, and everything in between, these imperatives are crucial to every modern security solution. And here's the kicker: If you aren't integrating these ideas at every step of your business and IT roadmap, you're doing more than just creating risk. You're failing to unleash the full benefits of a modern security solution. Consider this your call to action.

48%

of executives say security threats are evolving faster than security technologies.

– Avanade Hot Topics 2019

To learn more, visit: **www.avanade.com/SecureTheEnterprise**

1 You must make everything secure "by design"

Traditionally, enterprise security is treated like an afterthought, a "nice to have" feature in the course of digital transformation. Unfortunately, this approach leads to significant risk and becomes unsustainable as IT projects grow in scale and complexity. With the proliferation of the internet-connected devices on the edge, shared responsibility models with cloud providers, and the evolving workplace, security threats are everywhere. Failing to address them at every step of your journey, with a holistic approach, can be catastrophic.

The modern CISO knows security must be "by design." Take for example the emerging field of DevSecOps. In it, security is weaved into every stage of business application development, from initial design, to continuous testing, to authentication safeguards and industry best practices. Today's CISO must bring this by-design approach to the entire digital transformation strategy, the business at large. Security is no longer an afterthought; it's an integral thread of every IT and business initiative, ensuring you can move forward into the future, with confidence, agility and speed.

As few as 30% of organizations take cross-organization steps to drive a business-led approach to digital risk. – Gartner

To learn more, visit: **www.avanade.com/SecureTheEnterprise**

2 You must embrace emerging technologies

It used to be that emerging, transformational technologies – such as a migration to the cloud – caused alarm. In the traditional enterprise, IT was frequently seen as the "department of no," constantly pushing back and slowing the adoption of new technologies in an effort to maintain security. Meanwhile, the bad guys aren't staying still; they're using new technologies like artificial intelligence, automation and machine learning to up their game. Security leaders who reject emerging technologies will find they don't have the tools, or capabilities, to compete in a new world of risk.

The modern CISO knows security demands they embrace emerging technology.
As the bad actors get stronger, CISOs must not only keep pace but stay a step ahead. This can be a significant challenge for an enterprise with limited resources, but by partnering with industry giants and cloud vendors, such as Microsoft for example, they gain the advantage of billions of dollars in research and development spent every year on cybersecurity technologies and resources[1]. Only by embracing new technologies, and joining new partnerships and platforms, can CISOs adequately scale their security effectiveness.

Only 16%

of organizations report the capabilities of traditional security tools are sufficient to manage security across the cloud. – Crowd Research Partners

To learn more, visit: **www.avanade.com/SecureTheEnterprise**

[1] Reuters, "Microsoft to continue to invest over $1 billion a year on cyber security"

3 You must put identity at the center of security

The world of work is evolving. Data is on the move, being accessed and stored on the go, from a variety of devices, from a variety of locations. In this post-cubicle world, the model of placing all your data behind a static firewall is no longer practical. It's no surprise that a majority of today's data breaches are not caused by brute force perimeter invasions – they're coming from phishing scams and social engineering, credential-based vulnerabilities to get inside and cause trouble, according to CSO Online.[2]

The modern CISO knows identity is the new security control pane. Identity and access management (IAM) is the most effective way to ensure cybersecurity and resilience across an evolving, ever-changing landscape. In this new model, your users' identity is treated as a single point of control and visibility, which can scale and automatically adapt alongside your users, wherever they go. From automating "join, move, leave" operations, to using artificial intelligence to dynamically ensure good access, a solid IAM approach is the keystone to preventing data loss, maintaining control and protecting data for the modern enterprise.

Identity theft is the leading type of data breach, accounting for

64.5%

of all incidents in 2018. – Breach Level Index

To learn more, visit: **www.avanade.com/SecureTheEnterprise**

[2] CSO, "Identity Trends 2018: The More Things Change, the More Things...Change."

4 You must deliver a great user experience

CISOs ignore their responsibility for end-user experience at their own peril. Your users don't just want anytime, anywhere access to their applications and data; they want an engaging, frictionless experience. When security becomes too invasive or arduous to manage, end users start to look for ways around it. Human nature (read: laziness) threatens all security initiatives. And because human nature is nearly impossible to change, CISOs must evolve their thinking, instead.

The modern CISO knows security can't be a tax on the end user. They know an effective solution focuses not just on data protection, but on the needs and productivity of the user, too. With solutions such as single sign-on, biometric passwords and automation, modern security leaders are protecting their information by virtue of making applications easier and more intuitive to use. Creating a great end-user experience might feel like the job of marketers and sales, but CISOs must begin to appreciate – and listen – to this growing demand.

Only **33%**

of organizations are using single sign-on to secure and simplify user access. – Avanade Hot Topics 2019

To learn more, visit: **www.avanade.com/SecureTheEnterprise**

5 You must simplify the technology landscape

Chaos is a cybercriminal's best friend. As enterprises expand their boundaries, they create a jumble of ad-hoc, disconnected security solutions. This situation makes it challenging to gain visibility and take action on real-time security issues and breaches. Consider this: Enterprises are often running up to 70 different security solutions in their environment – yet breaches go undetected for 99 days on average, according to FireEye[3].

The modern CISO knows simplicity is power. As a result, they are looking to reduce their technological footprint, and gain a single, unified perspective on their entire environment, spanning cloud and on-premise workloads. Not only does simplification often create immediate operational savings, but it gives you the power to make informed, prudent decisions with more speed and accuracy. By leveraging automation and auditing security environments for opportunities to simplify or remediate an incident, modern CISOs are combatting the relentless complexity of the modern enterprise.

The complexity of IT environments is the most-cited security challenge by global security decision makers. – Forrester

To learn more, visit: **www.avanade.com/SecureTheEnterprise**

[3] FireEye, "Cyber Evolution: En Route to Strengthening Resilience in Asia-Pacific."

How to get started

Knowing what to do is important. Putting that knowledge into action is what matters most.

While the principles of modern enterprise security are easily boiled down to a few phrases and statistics, executing these new strategies pushes your business into uncharted territory.

Avanade can help put these ideas into action.

Whether you're leveraging the cloud, modernizing your workplace or concerned about data breaches, Avanade delivers the security solutions you need today, to succeed and grow tomorrow. We offer comprehensive security capabilities powered by end-to-end advisory, implementation and managed services and our deep expertise in the Microsoft ecosystem. Our holistic approach helps you:

- Create a roadmap to cybersecurity maturity
- Implement an effective, advanced and compliant cybersecurity strategy
- Drive productivity, collaboration and value to the bottom line
- Focus on innovation, not maintenance, with our managed services

To learn more, visit:
www.avanade.com/SecureTheEnterprise

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