FUJITSU

White paper

Customer-first security: What it is and best practices for success

It's always been important for Chief Information Security Officers (CISOs) to deliver value to the company's bottom line. But new demands are raising the bar much higher for CISOs.

Why Read This Paper:

It's always been important for Chief Information Security Officers (CISOs) to deliver value to the company's bottom line. But new demands are raising the bar much higher for CISOs.

The key to meeting those demands, retaining customers, growing business and keeping organizations secure lies in recalibrating security strategies for more integrated, big-picture thinking. It means keeping customer needs and business goals front of mind. It requires making better use of data for more proactive security insights and faster response times, as well as understanding the risks to customers so you can better prepare security programs for success. In the pages ahead, this white paper explores how you can achieve those objectives.

Introduction

The volumes of data generated today are exploding. More and more functions that were once managed in-house are moving into the cloud, meaning more of an organization's data extends well beyond traditional technology borders. This extended enterprise increases the already-massive potential for data leakage, data loss and regulatory compliance issues. Meanwhile, new data regulations are creating additional requirements to protect privacy and security.

These changes mean the threat landscape is continually evolving, making it hard for preventive measures to keep up. For CISOs, the pressure is on to make sure responses are immediate and are focused on protecting the best interests of their company's customers.

At the same time, C-suite executives understand ROI, not IPS (intrusion prevention systems). They want CISOs to view information risk as a business challenge, and to address that challenge as any other part of the business would do. That means defining security in terms of tangible business value that can be measured.

For you as a CISO, all of this means new responsibilities. You need to not only keep your company secure but also prove the business value that your team creates.

> The organizations best positioned to succeed in today's fast-changing environment will be those where security is part of the culture

That's because the organizations best positioned to succeed in today's fast-changing environment will be those where security is part of the culture, where it aligns with enterprise goals while keeping customer needs at the forefront at all times. In short, security must show how it adds customer value to contribute to the organization's bottom line.

What's the key to meeting these challenges?

It comes down to recognizing that security involves far more than technology. A truly effective security strategy ensures the business can deliver its products and services in a way that customers trust – not just for the value of security alone, but also for a positive business impact. Without customer trust – the foundation for a company's brand and reputation – no organization can stay in business for long.

> Without customer trust – the foundation for a company's brand and reputation – no organization can stay in business for long.

The elements of customer trust-based security require digital oversight and risk management, not just technology.

Growing proportions of consumers have indicated they do not trust organizations with their data. In the consumer space, studies have shown that loss of trust can lead users to abandon a brand after a data breach. For that reason, CISOs must take reputational risk seriously and build a risk management framework that sustains evolving business models while also building and retaining customer trust. This requires technologies, people and processes that ensure availability, reliability, integrity, confidentiality, privacy and safety, as well as resilience. But it requires the right mindset as well.

Prioritizing trust means embedding a data privacy and security mindset organization-wide, not just in IT. It also means focusing on the ROI of your security strategies by proposing security objectives that protect reputation, help reduce everyday operational costs and increase customer trust, as these all support business retention and expansion. Business relies on trust, and trust requires security.

As security becomes ever more integrated into the successful running of a business, CISOs must map everything into a business context that is relevant to the board and shareholders, while at the same time avoiding issues that are relevant only to IT decision making. This shift in thinking delivers benefits beyond security alone. It makes it easier for organizations to work better, innovate faster, deliver projects more quickly at lower costs, and delight customers. In short: it's a must for digital business.

Roadmap to intelligence-led security and customer trust

In the emerging era of digital business, the traditional approach to security is no longer enough. Today, managing risks means paying attention to a vast amount of security activity and data – internally, across networks and in the cloud. That information can say a lot about past, present and future threats, and about how to make the best possible decisions for the business and its customers.

Making sense of such data requires an organization-wide recognition of security's importance to the company's success. It's all about gaining an enterprise view, a big-picture vision of security that produces a more nimble, resilient and customer-focused business. It ensures that security is in your DNA.

How do you enable such a shift? While a risk-based and intelligence-led approach to security requires continuous effort and adjustments as circumstances change, the following roadmap will help get this strategy under way:

1. **Start with your business goals**. This involves answering questions such as, 'What is my organization's reason for being?', 'What is it trying to achieve?', 'What problems does it solve for customers and how does it do this?', 'What is the customer experience like?' and 'What about those customers' customers?' Once you've clarified what it is you're trying to achieve, you can begin planning how to get there.

2. Then **think about how security enables these goals**. What data is used or generated in the course of pursuing these objectives? How does that data need to be protected? What systems and practices are needed to make this happen? Be sure to consider not only data provided by customers but data that's produced and used during development, manufacturing and shipping, as well as during daily operations. It's also important to think about how the customer experience relates to data security and privacy concerns.
3. Building on this, **identify your security objectives to enable the larger business goals**. Think about the new capabilities you'll need, and what kind of governance will be necessary to ensure new processes are properly managed. Pay attention to data requirements for regulatory compliance, too. These can vary, depending on the markets and regulatory regimes in which your business operates.
4. You should also **think about other projects, programs and applications that could come into play**. For example, if one of your organization's goals is to become more mobile-friendly for customers, how could the introduction of new user apps affect compliance with data privacy and protection regulations in different markets?
5. Another key step is to **identify potential stakeholders who might have a say in your security transformation**. Who needs to be consulted or informed? Whose support is needed? Who will be responsible and/or accountable? These could include everyone from internal marketing teams to outside technology partners, equipment manufacturers and app stores. It's critical that all relevant stakeholders are involved, because their trust – whether it's shareholders, employees, consumers or someone else – is essential to business success.
6. Then **think about what other actions are needed to ensure your security goals are met**. For instance, the rollout of a new customer app in regions covered by the EU's General Data Protection Regulation might require your organization to designate a Data Protection Officer if you don't already have one, or to set up new consent mechanisms for app users.
7. From there, **establish the specific outcomes you'd like to achieve** while working toward your business and security goals. For example: 50,000 active app users with the right levels of privacy, safety and security by the end of the fiscal year.
8. As you follow this roadmap, be sure to c**onsider how achieving your goals and outcomes might affect the maturity of your security operation**. For instance, driving rapid adoption of a new consumer app could require the hiring of additional developers and the adoption of faster development cycles.
9. Finally, **decide how your security organization will track and measure progress** toward achieving business goals. By linking security KPIs to wider company objectives, you ensure that security and business strategies are well aligned. Say your business is launching a new B2B e-commerce site and aims to sign up 1,000 new clients over the next 12 months – the security team could monitor a related metric, for example, by tracking how many of those users opt to use biometrics instead of passwords to log in.

By considering many different aspects of security and risk management, these steps pave the way for better, more insightful and more business-aligned security. They also underscore how security in the digital age is about much more than technology alone. To be sure, CISOs following this roadmap for transformation also need to watch for gaps that need fixing. But building a security culture that's always watching for risks and ways to manage them is vital. Once these objectives and measures are in place, it's also important to continually assess whether they are still right as the security landscape and business needs change, to avoid these measures becoming irrelevant.

It's critical that all relevant stakeholders are involved, because their trust – whether it's shareholders, employees, consumers or someone else – is essential to business success.

What's in it for you? How business-aligned security helps CISOs

Aligning security strategies to wider business objectives makes life better for CISOs in many ways. It builds greater awareness of the importance of security across the business and can help pave the way for the creation of security champions across the organization by linking effective security to business success as a whole.

Among the benefits you'll discover:

- **Wider organizational support** – Better, big-picture understanding also makes it easier to communicate concerns with other business stakeholders, which improves the potential for cooperation. This provides better context on how security issues affect different parts of the business. In addition, wider support for security matters makes it easier to get buy-in for awareness campaigns, training and prevention programs… and other investments. There's a mistaken notion that CISOs alone are responsible for organizational security, when in fact everyone in the company must play a part.
- **Simplified security** – Many businesses deploy far more security technologies than they need because of siloes across different departments, business units and office locations. Approaching security holistically allows for businesses to determine the best approach that fits with their enterprise architecture, but it can do more than streamline technology, too: it can also pave the way for automation, freeing people to concentrate on more rewarding, innovation-focused activities to drive competitive advantage. While transforming security operations can be complex and challenging, the longer-term result is simpler, smarter and more efficient security.
- **Better insights for planning** – A more business-focused approach to security also makes it easier to fine-tune strategies for an organization's unique needs. This enables security to become more mature and forward thinking, rather than ad hoc. Setting targets – "We want to be here in three to five years" – is an essential part of this. Of course, circumstances will change over time, so this process must remain flexible and adaptable for continuous development.

- **Budget benefits** – By demonstrating how security contributes to improved revenues and other benefits, you will find it easier to make your case to executives during budget planning and to gain support for security investments from business stakeholders. Focusing your cybersecurity strategy on customer trust also promotes support for greater funding for technologies to attract and retain customers.
- **More recognition of security's value** – Board-level executives want to know the business impacts of security risks and investments. When CISOs can go beyond the usual technical topics and communicate what security does in terms of risk management, brand protection, customer trust, privacy, data governance, third-party management and more, they demonstrate its value to wider parts of the business.

These are all concrete, real-life returns on investment for CISOs who choose to transform their organizations.

> There's a mistaken notion that CISOs alone are responsible for organizational security, when in fact everyone in the company must play a part.

Overall benefits of business-focused security

C-suite executives have many reasons to welcome a security transformation too. Businesses where security is everyone's business, when it's well aligned with company goals and customer needs, reap clear advantages in the emerging digital environment.

Improved security thinking means fewer breaches. When breaches do inevitably occur, it means faster response times, fewer (or less severe) negative impacts, better lessons learned and improved resilience.

This means businesses are more compliant with data privacy and security requirements, and face fewer regulatory fines and fewer damaging news headlines.

In addition, organizations where security is baked in encounter fewer stumbles in new projects and initiatives. When development of new products and services takes security into consideration from the start, there are fewer "back-to-the-drawing-board" delays. This speeds up time to market, helping businesses move faster than competitors.

> Intelligence-led security ensure that customers' data, privacy and security are taken seriously. This cultivates trust and contributes to the company's brand and reputation. It encourages customers to remain customers, rather than looking for alternative places to do business.

Last but not least, all of the preceding benefits of intelligence-led security ensure that customers' data, privacy and security are taken seriously. This cultivates trust and contributes to the company's brand and reputation. It encourages customers to remain customers, rather than looking for alternative places to do business.

> While transforming security operations can be complex and challenging, the longer-term result is simpler, smarter and more efficient security.

Future security and the next generation of CISOs

All of the steps outlined above represent a work in progress. Security is a continually evolving process. It's never "done". However, that doesn't prevent you from moving forward. Ideally, you should focus not just on where you'd like to be today or a year from now but on where the business should be over the longer term. That's vital for companies to remain viable, successful and profitable in tomorrow's more digital and connected society.

The next generation of CISOs must move closer to business management. It needs to fundamentally understand industry business processes, regulations and risk beyond just technology.

Making security a priority involves not only regular training and testing – the occasional dummy email to check for phishing awareness, for example – but a constant drip-feed of information. The goal is to get people thinking about security at work as much as they might at home, where most of them (hopefully) make a habit of locking their doors, leaving a light on at night and avoiding letting strangers in.

Building a security culture means cultivating security champions across the organization, avoiding complacency and "tick-box" thinking, and fostering an environment where people aren't afraid to report mistakes. It also requires nurturing a diverse security team with a range of abilities and talents – people skills, technology skills, communication skills, business skills and more. So think about in-house apprenticeships and partnerships with educational institutions and professional associations.

Most of all, look for people who can step into the CISO's shoes down the road and who share your vision of customer- and business-focused security. Whatever changes the future brings, your organization will always need to protect customers' best interests.

Conclusion

Today's security demands are vastly different from those of the past – and they'll keep changing with the emergence of new technologies, new business models, new threats and entire new industries and needs. Nevertheless, the fundamental role of business security will always remain the same: to ensure and retain the trust of customers and other stakeholders so the company can stay in business and continue growing.

To embed this mindset in your organization, remember the following:

- As a CISO for this digital era, you must manage information risk and focus relentlessly on the customer if you want to maintain budget and authority, and gain relevance. Focusing on risk and customer needs is also essential for gathering, analyzing and understanding the right cybersecurity metrics for your business.

- Focusing on overall business goals and customer needs lets you demonstrate the value of security and contribute to the company's bottom line. Beyond technology, security requires digital oversight, risk management, intelligence, insight and transparency. Enable this through centralization for a single-pane view of activities, needs and risks, and by embedding security thinking into everything your company does.
- Security is never done – it requires continuous effort to build awareness and adapt as needs change. However, you're not alone: security concerns everyone, so you have an entire organization of potential champions who can contribute to the effort.
- Paving the way for future security requires planning, adaptability, flexibility and diversity – tomorrow might bring new business models but it won't change the fundamental *raison d'etre* for businesses: to serve customer needs. What's more, customer-focused security is good for everyone else as well – CISOs, security teams, product development teams, other stakeholders and the business in general – because it keeps the focus on human needs.
- While security involves far more than technology alone, technology is a great enabler. Thanks to the cloud and as-a-service options, solutions are easier, more affordable and more accessible than ever to businesses of all kinds.

The fundamental role of business security will always remain the same: to ensure and retain the trust of customers and other stakeholders so the company can stay in business and continue growing.

Ultimately, your goal as a CISO is to help everyone in the company – from the CEO and executive board on down – to understand that security is a business enabler, and that it's not just a cost center but a revenue generator. It's the opposite of being the security leader whose only answer is "no", which makes it hard for others to see you as a business leader. You demonstrate real leadership by getting in front of your organization and showing how you can increase revenue and profitability.

Want to learn more about how to transform security for a greater focus on customer and business needs? Fujitsu's approach to intelligence-led security can help with advice, monitoring services, infrastructure services and more. Visit www.fujitsu.com/emeia/themes/security/ , contact us at +44 (0) 1235 79 7711 or email askfujitsu@uk.fujitsu.com to learn how to get started today.

FOLLOW US on LinkedIn and Twitter @FujitsuSecurity

About Fujitsu Security
As a global security service provider, Fujitsu provides security and resiliency solutions across the full IT delivery lifecycle, integrated within the operational, service and security framework within an organization; Fujitsu is an extension of in-house security capabilities. The diversity of customers and partners that we work with gives us an in-depth understanding of differing security requirements across industries and geographies, while our advanced threat capabilities provide a comprehensive view of the ever-changing cyber threat landscape.

We leverage 40-years of experience and investment in cyber security R&D to bring new ways of thinking. This means intelligence-led solutions to cyber security challenges– all delivered to the highest security standards – helping customers build a cyber security capability that demonstrates true business value and enables business innovation.

Our wealth of intelligence and experience allows customers to be predictive and proactive, and our consultancy services and solutions keep you ahead of new and unexpected threats. All of this means that you can be primed and ready to mitigate risks, helping your business focus on opportunities to create value – securely.

Here's why you should consider Fujitsu:

- Fujitsu has achieved recognition from Gartner, the leading independent analyst firm, as one of the global leaders in Managed Security Services
- Our holistic approach to security works to combine human intelligence, through our highly-skilled analysts, with technical intelligence using Machine Learning, advanced analytics tools and best-of-breed security technologies to deliver 24/7 support
- Thanks to our intelligence-led approach, we provide tailored solutions, giving you the ideal response to constantly shifting security challenges
- The strength of our proven experience, vendor relationships, and global scale means that we're well placed to optimize your approach to security, and provide real-time intelligence and visibility on the state of your IT environment
- We offer security services that meet compliance demands and align with security policies such as PCI DSS, ISO 27001/2, SOX and ISO22301:2012.

For more information, please visit https://www.fujitsu.com/global/themes/security/

Contact
Ask Fujitsu
+44 (0) 123 579 7711
askfujitsu@uk.fujitsu.com
@FujitsuSecurity
Ref: 3938

www.fujitsu.com/global