AGENTS OF CHANGE

HOW EXECUTIVE LEADERS CAN SECURE NEW CHANNELS TO DRIVE BUSINESS INNOVATION

SAFEGUARD CYBER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

FEWER THAN 25% OF EXECUTIVES

SEE INFORMATION SECURITY AS AN ENABLER OF DIGITAL TRANSFORMATION

IT'S TIME FOR A

RADICAL CULTURE CHANGE.[1]

EXECUTIVE SUMMARY

While digital transformation is debated in boardrooms and over team meetings, nimble startups are emerging to disrupt entire industries. New apps, services, and brands storm media headlines almost daily to challenge the dominance of traditional enterprises. Technology adoption around digital channels -- social media, mobile apps, and collaboration networks -- represents the frontline of a digital revolution that cuts two ways. The same decentralized and distributed landscape that empowers users to text friends on the other side of the planet also poses significant security risks for centralized corporate enterprises. The businesses that negotiate this paradox will be the winners. Those that hesitate will be disrupted or left behind.

A recent study by McKinsey found that 84% of business leaders agree that innovation is a key priority, yet only 6% are happy with the results.[2] A pervasive reason for this misalignment is the fact that most people still consider information security to be an impediment to innovation. IT is commonly perceived as creating restrictions that create barriers to productivity and customer success alike. However, it's not all IT's fault. In fact, many of the world's largest companies are being held back by this sort of siloed thinking.

On the one hand, new social and digital technologies pose challenges for information security and risk teams. But on the other hand, the traditional mission of IT or the Chief Information Security Officer's (CISO) has been to guard the fortress through a mix of policy enforcement and cautious adoption. The current cultural shift toward digital transformation is applying pressure for faster innovation. This pressure is compounded by the fact that by now, employees accustomed to using social media, mobile devices, and collaboration networks in their personal lives, and want to use these same channels in the workplace.

This paper will look at how:

- Information security can be a business driver, not just a cost center
- The responsibility for security now belongs to all departments, not just IT
- Organizations can better prepare for the future of digital business

It's time for a radical change in thinking and corporate culture. Executive leaders must now viewing security as an enablement tool for innovation, not simply a technical risk. The choice between innovation and security is a false one. Instead, executive leaders should be thinking about measures that let end users use modern platforms like social media and online collaboration tools to improve business outcomes.

HOW INFORMATION SECURITY CAN DRIVE BUSINESS FORWARD

1/3

"A THIRD OF BUSINESS LEADERS

now consider information security to be a driver of competitive advantage, differentiation, and increased business efficiency."[3]

"60% OF CISOS

claim that data breaches are changing business leaders' attitudes about their security strategies" [4]

"31% OF BUSINESS EXECUTIVES

consider the first priority of cybersecurity to be growth enablement, while the remainder still see the main purpose as risk reduction." [5]

Most people are so accustomed to using social, mobile, and collaboration apps that it should come as no surprise that enterprise employees expect the same degree of freedom and convenience in the workplace, too. Sales teams, for example, often use social media to boost visibility, while remote employees keep in touch with one another through online collaboration platforms. While security and privacy are growing concerns, it's unlikely that any workforce will completely stop using these technologies, whether they're approved or not. In fact, a study has shown that while 70% of people are concerned about online privacy, fewer than 40% ever bother to read privacy statements.[6]

As perceptions of information security and online privacy evolve, people are looking for trust signals that let them use technology in confidence. Instead of being seen as a compliance hurdle or cautious supervisor, information security should now be seen as a driver of competitive advantage and increased business productivity. When teams aren't permitted to engage with customers on LinkedIn or collaborate with overseas partners over WhatsApp, for example, an enterprise erects artificial barriers. In the case of WhatsApp, it is the digital native communication channel in critical overseas markets like India and Brazil. Forcing teams to use only approved applications like email is like a French multinational insisting its workforce speak only French in its Mumbai office. That decision would be unrealistic and impede business. More importantly, this kind of decision-making neglects a business opportunity.

Digital communications -- customer care teams chatting with customers, sales teams texting clients, teams collaborating internally -- contain risks yes, but they also contain valuable insights around improved products, processes, or ideas. And the scale of data magnifies both the risks and insights. During a pilot program with one of our clients in Brazil, thirteen sales reps produced more than 2,400 messages with customers and prospects in only 14 days. Sales reps felt unshackled, and they were able to communicate faster and more naturally than had the company insisted only on approved email channel. Obstacles to digital adoption will, at best, hamper productivity, and at worst, leave opportunities for more nimble competitors to seize market share.

When information security gets in the way of workflow, employees will likely look for workarounds, however risky. The same applies when employees are faced with reams of complex documentation and complicated security controls. Given that human error is the number-one cause of data breaches, it's of utmost importance that security solutions are easy to use and are themselves enablers of the systems they protect.

Today, executive leaders must lead a culture change that transforms the perception of information security from a hindrance into a driving force of better productivity, efficiency, and confidence across all departments. This will require greater cross-department discussion and collaboration around what technology and channels will help teams perform better. For example, does the CMO want more social media channels enabled? Is the Head of Compliance holding the CRO's sales team back from using WhatsApp? The conversation must also address risks. What controls does that same CMO have in place to archive and protect customer interactions over social? Does the CRO have a clear view of mobile conversation for legal exposure? It's time to break down silos and embrace the idea that information security is not just an IT concern. It's a primary business problem.

INFORMATION SECURITY IS EVERY DEPARTMENT'S RESPONSIBILITY

ONLY 44% OF CISOS

BELIEVE THAT EXECUTIVE LEADERSHIP CONSIDERS THEIR ROLES A POSITIVE FORCE IN INNOVATION.[7]

INFORMATION SECURITY IS EVERY DEPARTMENT'S RESPONSIBILITY

Traditionally, CISOs and IT departments have been encouraged to adopt a citadel protectionist mind-set. However, this sort of conservatism in today's enterprise will only result in conflict. But again, blame doesn't fall to the CISO alone. There's also the issue of teamwork. Although perceptions are changing, information security has long been seen as a technical challenge. The burden of information security often falls to the CISO and IT teams, and to them alone, rather than being considered something that's everyone's responsibility.

NEW ROLE OF THE CISO

Over 80% of security professionals believe social media, mobile messaging, or collaboration apps present medium to high risks to their organization - *SafeGuardCyber Survey April, 2019*

Executive agents of change must make clear the information security responsibilities and accountability of everyone in the company, lest it risk falling back into silos and the crippling inefficiencies that come with them. To break out of the tech silo, executive leadership needs to drive a change in thinking that gets business leaders to own risk. That starts with gaining command of the facts:

- Get full visibility into information assets to support a company-wide risk profile
- Reach a consensus with stakeholders on key priorities and the impact of compromise
- Develop a strategy whereby the adoption of new technologies is secure by design

CISOs should never have to work alone. Rather, departments needs to collaborate throughout the business. Information security should be embedded into all business processes, ensuring that everyone on the team is accountable to one another. This may take the form of exercises and simulations, but they must mirror real-world processes. For example, if sales teams conduct business LinkedIn, then phishing awareness programs need to include Direct Message spear-phishing scenarios, not just email. Has marketing been trained on social media account takeovers? Has compliance been trained to find risk-bearing language on internal chat channels?

BECOME A ROLE MODEL FOR DIGITAL TRANSFORMATION

Only 20% of security professionals feel confident they are effectively mitigating the digital risks from social media, messaging and collaboration apps. - *SafeGuardCyber Survey April, 2019*

In addition to having a high level of technical expertise, CISOs need to partner with other department heads to develop a thorough understanding of how the business model works. In fact, they should be running information security like it's a business. To do that, they need to have influence at the board level, their number-one goal being to drive the adoption of new technologies, safely and securely, that contribute to business goals such as lead generation or access to new markets. Today's business processes demand that all enterprise executives become mentors, leaders, and role models for technical innovation.

Influence comes with confidence and, when it comes to confidence in information security, the CISO must be fully informed with the facts and strategically prepared. To stay focused on this high-level role, they should consider outsourcing non-strategic elements. Instead, they need to lead a change in thinking by focusing on key operations like technology alignment, baselining, and advice to board members.

BUILDING ENGAGEMENT ACROSS LEADERSHIP TEAMS

35% of businesses provide verbal guidance or in-person training, on the potential risks of using third party apps in a business context. - *SafeGuardCyber Survey April, 2019*

Senior executives must clear the lines of communication, and break down organizational barriers that put the twin demands of security and innovation at odds with one another. To make that happen, they need to have support across the organization. The information security department can no longer stand alone. Its mission and priorities are now intrinsically intertwined with sales, marketing, development, customer support, and every other critical business function. That role means CISOs must speak in a language that everyone else can understand, and determine how they can add value across the organization. It also means that other departments need to discuss the business imperatives and risks for new channel adoption and work more closely with security teams. While matters of security, privacy, compliance, and governance remain top priorities, it's also important how teams communicate these challenges. To that end, everyone within an organization should be thinking of security in terms of how new technologies can:

- Differentiate the business from its competitors
- Empower employees to work smarter
- Drive better operational efficiency
- Generate and protect revenue

As the organization's subject matter expert on information security, CISOs should be proactive in sharing knowledge across the company. Whether it's news about the latest data breach or the latest technology trend, an important part of the new role is keeping executives informed. If, for example, a data breach or security vulnerability affects a major cloud provider, business leaders will want to know if and how it could affect their operations. Similarly, if frontline teams are sharing feedback about the channels that customers and prospects prefer, they must be transparent with the CISO.

LEAD BUSINESS CHANGE WITH STRATEGIC PLANNING

Only 31% of organizations have a documented process for requesting a new app to be added to the approved list. - *SafeGuardCyber Survey April, 2019*

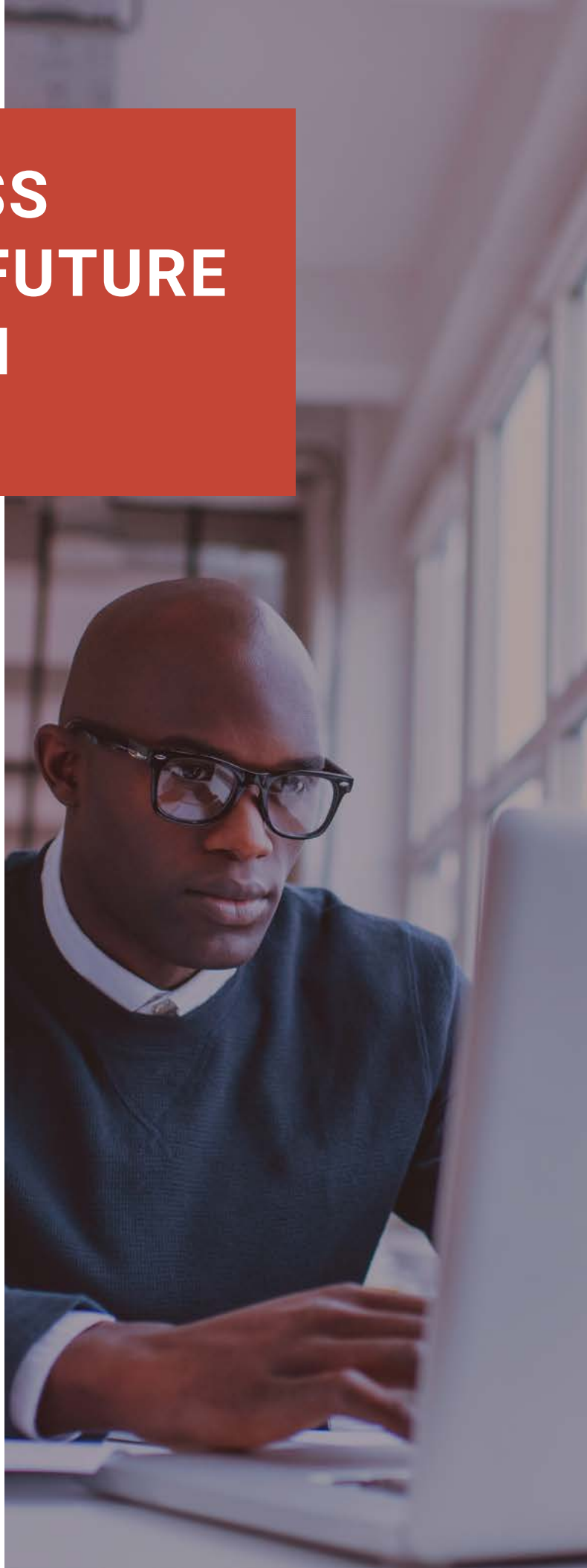
Information security is no longer just an IT issue. It's an enterprise risk that affects every employee and every customer and, ultimately, the viability of the organization. Executives who lead business change do so by sitting down in the boardroom to give their fellow executives the confidence to make informed decisions around innovation and risk. They can bring the risk closer to home by conducting simulations, but it's equally important that everyone around the table knows that the business cost of not using modern technology is often even higher than innovating quickly. Some studies placing the cost of failing to innovate at a 24% reduction in profitability.[8]

One of the best ways to lead business change is to embed information security team members in all core business processes. In larger companies, CISOs should delegate certain operations to specialists in each department who, in turn, report to executive management as part of an overarching information security strategy. This approach will not only help ensure that all corporate assets are accounted for; it will also help simplify risk management to drive faster innovation. By engaging with every facet of the organization, security teams will be better placed to lead business change and establish long-term development goals that help transform information security from a mere necessity to a growth enabler.

IS YOUR BUSINESS READY FOR THE FUTURE OF INFORMATION SECURITY?

“73% OF ORGANIZATIONS ADMIT THEY’RE STILL UNPREPARED FOR A CYBERATTACK.

DESPITE CHANGING ATTITUDES, THE LINE BETWEEN INNOVATION AND GOOD SECURITY PRACTICES IS WIDER THAN EVER.”[9]



IS YOUR BUSINESS READY FOR THE FUTURE OF INFORMATION SECURITY?

Risks and cyber threats evolve as new vulnerabilities arise and threat vectors diversify. Attack surfaces expand as businesses move beyond internal IT to take advantage of collaborative cloud and mobile technologies and social media. Today, an organization's employees are the attack surface, not just IT hardware and infrastructure. However, to be ready for the future of information security, businesses need to have an overarching strategy that goes beyond conventional perimeter defense to add an external layer of protection against data loss, insider threats, VIP exposure, digital endpoint vulnerabilities, and ultimately brand damage.

Forward-looking executives will drive necessary change by putting the power in the hands of everyone concerned and helping create a culture of accountability across the entire organization. Instead of fearing a reprimand from IT, employees will be empowered by the ability to report threats themselves. Senior management will quickly see the benefits in the form of a more engaged and empowered workforce, greater confidence among employees and customers alike, and increased operational efficiency. All these things together can bring enormous value to the company.

FINAL WORDS

As businesses strive to keep pace with evolving customer demands, they are under constant pressure to adopt a proactive stance to information security with continual improvement and security by design. To summarize, executives can position themselves to offer greater business value by:

- Driving a corporate culture change in which security is everyone's responsibility
- Building relationships with every department to overcome organization silos
- Moving away from the department of "no" to becoming innovation leaders
- Leading business change with strategic planning

To help make life easier for today's connected executives, we developed SafeGuard Cyber to empower organizations to use social media, mobile chat, and digital channels securely, compliantly, and at the scale of global business. With coverage across 50+ channels, such as Facebook, LinkedIn, WhatsApp, Slack, and Office 365, our clients unlock new markets and reach new customers, all while securing customer interactions and company data. It's no longer a matter of saying 'no' to new digital and cloud technologies. It's about asking 'how' an enterprise can embrace new technologies without fear.

SOURCES

1 https://www.bromium.com/wp-content/uploads/2017/10/The-CISOs-Dilemma-Infographic-Bromium-October-2017.pdf

2 https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/how-we-help-clients/growth-and-innovation

3 https://www.capgemini.com/nl-nl/wp-content/uploads/sites/7/2019/01/The-Modern-Connected-CISO-5.pdf

4 https://interact.f5.com/2019ALLFCISOResearchMarketoPage_CISOResearchReport.html

5 https://www.newhorizons.com/Portals/278/Downloads/Cybersecurity-as-a-Growth-Advantage-Cisco.pdf

6 https://www.researchgate.net/publication/325332842_A_CYBER_DOMAIN-SPECIFIC_RISK_ATTITUDES_SCALE_TO_ADDRESS_SECURITY_ISSUES_IN_THE_DIGITAL_SPACE

7 https://www.computerweekly.com/news/252456376/Business-failing-to-see-strategic-value-of-cyber-security

8 https://www.capgemini.com/gb-en/wp-content/uploads/sites/3/2017/07/The_Digital_Advantage__How_Digital_Leaders_Outperform_their_Peers_in_Every_Industry.pdf

9 https://www.inc.com/adam-levin/more-than-70-percent-of-businesses-admit-theyre-unprepared-for-a-cyberattack.html

SAFEGUARD CYBER

Americas
410A East Main St.
Charlottesville, VA 22902
USA

+1 (800) 974-3515

sales@safeguardcyber.com

Asia-Pacific
PO Box 523
Leichhardt NSW 2040
Australia

+61 (437) 276-739

APACsales@safeguardcyber.com