Making cybersecurity a core business priority

Financial services cybersecurity webinar summary
Introduction

The changing disruptive landscape and frequency of cyber attacks throughout the world present serious challenges for the financial services industry. Less than 14% of financial services respondents to EY’s Global Information Security Survey 2017 think that their information security function fully meets their organization’s needs. Cybersecurity is no longer simply an information technology (IT) or compliance issue; it is a core priority that requires a new business approach.

On 25 May 2017, EY hosted a cybersecurity webinar, *Why cybersecurity is everyone’s responsibility in today’s financial services organization*, to explore key issues that are foremost in the mind of the C-suite. The webinar focused on the global cybersecurity landscape, and the threats and opportunities facing financial services organizations. The Panelists also reflected on the implications of the General Data Protection Regulation (GDPR), which is particularly relevant since firms have only one year until the official implementation date. This paper summarizes the discussion from the webcast.

Steve Holt, EY EMEIA Financial Services Cybersecurity Leader, chaired a panel of EY’s EMEIA Data Protection and Privacy Leader and two major global banks that have day-to-day responsibilities for managing cyber, data protection and privacy across their organizations. This includes developing strategies to integrate cybersecurity with risk management and IT, as well as collaborating with customers, suppliers and vendors. The webinar provided an opportunity to share knowledge and lessons learned in an informal setting.

Panelists included:

- **Cheri McGuire**, Group Chief Information Security Officer, Standard Chartered Bank
- **Simon Hales**, Group Head of Information Security Risk (ISR), HSBC
- **Tony de Bos**, EY EMEIA Financial Services, Data Protection and Privacy Leader

The discussion focused on four topics that this paper summarizes:

1. **Awareness and talent** – building a culture that makes cybersecurity part of everyone’s job, and rethinking the role of the chief information security officer (CISO).
2. **Innovation and risk mitigation** – putting cybersecurity at the heart of business strategy, to help ensure that new digital innovation includes cybersecurity at the outset and mitigate risks.
3. **Regulatory implications** – assessing the impact GDPR will have on your organization’s people, processes and technology, ahead of the 2018 implementation date.
4. **Resilience and scalability** – being prepared to recover rapidly from a cyber breach while holding your ecosystem to the same cybersecurity standards that you follow as an organization.
Where does the cybersecurity function sit within an organization?

As cybersecurity roles evolve and expand, there is a changing orientation of security functions. Historically, cybersecurity’s proximity to other security functions has not been static and will continue to emerge as an integral business risk. The panelists predicted that this will occur within the next two to three years.

Responsibilities will also change as cybersecurity matures from a discrete function into more of a cross-sector discipline. When Simon Hales started at HSBC, the security team was within the risk function, having moved from IT years before. Within a short time, accountabilities were realigned, and capabilities were reassigned back to IT, where it had a greater sense of ownership and was a better organizational fit.

While the panelists agree that IT, risk and operations are inseparable, the path is not straight. Security functions need to stay connected on all levels, despite the hurdles. Since 2013, nearly one-third of our survey respondents cite a lack of awareness and support as hindering the effectiveness of cybersecurity. Communication must begin with each project and be articulated on all levels.

“Communicating and having access to the board is important – and some organizations have not yet established these internal relationships,” Tony de Bos, EY.

Addressing the skills gap

One of the top three challenges is not having enough staff with the right multidisciplinary skills to manage changing roles. There is plenty of talent out there, but is that talent matching the needs? There are gaps within the workforce of seasoned professionals – those who can manage beyond a single area of knowledge. To fill those gaps, organizations need to look at other non-technical disciplines as a source of talent.

The skills gap is not trivial. It is one that affects most organizations in building capacity within this space. The private sector has a part to play here, which has yet to be realized. The pipeline for talent generation may take another decade to catch up. Larger organizations have graduate training programs and schemes, but many do not equate the need for security on the same level as other business functions.

“Cybersecurity has not traditionally been viewed as a multidisciplinary profession. Given the breadth of capabilities needed to manage risk, it requires a whole spectrum of training and skills development.”

Cheri McGuire
Group Chief Information Security Officer
Standard Chartered Bank
Innovation and risk mitigation

Security can help enhance innovation

Financial services organizations are adapting in new ways, and the speed with which they are rolling out new products and services is accelerating. A customer life cycle that took one or two years can now take only a few weeks. That requires companies to pivot the way they develop and roll out their products – overcoming the challenges by becoming more nimble and agile. It is a massive opportunity to embed security thinking within organizations. Building security as a pillar within an organization can actually enhance innovation.

“Data security and cybersecurity go hand in hand. The opportunities far outweigh any security risks, obstacles or threats to the brand. If people understand the risk appetite, they are better informed to make the right decisions quickly,” Tony de Bos, EY. Organizations need to have a multidisciplinary process in place, understand data flows and put effort into reducing their risk profile.

“The threats we face are very disruptive to an organization. Security has gone beyond protecting information. The function needs to be more strategic and responsive, while embracing new technology and becoming more mobile.”

Simon Hales
Group Head of Information Security Risk (ISR), HSBC

Security risk mitigation

Cyber is a business issue – not simply a technical or risk issue. And, as time plays out, organizations will be required to meet certain benchmarks and security levels. A big part of financial services revolves around security risk mitigation and the use of security vendors.

The panelists agree that some third parties are not doing enough to protect the organizations they work with – in other words, the buyer needs to beware. Third-parties are running an organization's brand, and sometimes, the lines blur on where they stop and start. Managing third parties should be viewed more holistically, with a risk-oriented approach. This requires a security review at the start of the process and continual monitoring.

“We are moving toward real-time security monitoring of third party vendors and becoming informed about the increased risk. The threats are changing and third parties need to understand this too. Ultimately, we cannot outsource risk – we own it,” said Cheri McGuire, Standard Chartered Bank. The level of awareness has to be an elevated topic within any organization.
Regulatory implications

Preparing for GDPR
GDPR comes into effect in 2018 and, for many firms, implementation will be a challenge. Organizations need to be doing more to prepare for it. A few companies started a year ago and have a credible plan in place, but most are only now kicking off their programs and searching for the right multidisciplinary team of lawyers, technicians, risk managers and data specialists.

“GDPR is not just another regulation or standard. It is a real business issue that impacts all key processes, and requires new and existing cybersecurity products to be compliant.”

Steve Holt
EMEIA Financial Services Cybersecurity Leader
EY

To implement GDPR, companies need to understand their data flows, which many do not, and start mapping them to see if they are compliant. This is important because GDPR takes a risk-based approach, rather than a compliance.

“Data sharing is a key component of this regulation, and it takes a lot of effort for an organization to be compliant. We have seen great data analytics initiatives for adding value, but these are not compliant with GDPR,” Tony de Bos, EY.

Most financial services firms have separate programs to link GDPR with banking initiatives. It is important to connect the dots and align them with business strategies. Communication is key. “The level of awareness has to be an elevated topic within your organization, and the board needs to be briefed on all regulatory challenges,” Cheri McGuire, Standard Chartered Bank.

Working with the regulators
Simon added that there are different flavors of regulation and it varies by region. “If I step back, I can see that most regulations are well intended, but there are differences. Those can be worked through, but what keeps me awake is meeting the deadlines – which comes down to project management.”

To succeed, organizations need active support from management, communication on the scale of the impact and cost governance. While cloud requirements and guidance from regulators may be costly, they have to be considered. Regulators demand that companies be transparent in data and risk. It is important, from a security view, that organizations engage with regulators, influence their thinking, and discuss what is practical and achievable versus unreasonable.
Preparation for and responding to cybersecurity attacks
With the threat landscape continuing to change, organizations need to improve and become more resilient in daily activities and planning for potential events. The panelists agree on the need to have systems in place around response and recovery. Resilience is not just whether a business can withstand an attack. It is also about how the organization responds and how the crisis team reacts to restore service offerings. Resilience encompasses many diverse activities.

A number of companies perform exercises that build awareness and look at the whole spectrum of preparedness. This involves both the crisis and management team, communication to address external requests, and the board acting to protect shareholder value. Organizations and teams that thought war-gaming activities were unnecessary have shown that they were able to learn and benefit from the training, and be better prepared for potential cyber attacks as a result. Tony de Bos, EY reiterated that “One cannot practice enough – and practicing demands leadership from boards.”

Cybersecurity is everyone’s responsibility
Security has to be embedded across the business, and no longer viewed as an IT component. Once a business-driven plan and processes are in place, there needs to be awareness, training and an understanding of the shared roles of responsibility and accountability.

“For cybersecurity teams, if you are looking at a problem from a technology perspective, you have it wrong. You need to think much broader – and, if you are only talking to your technicians, then you definitely have it wrong,” Simon Hales, HSBC.

“Do not take data and infrastructure for granted. Security must be built into every product and service. It is a three-legged stool of people, process and technology. All three are critical. If one is missing or weak, you may have a significant security gap.”

Cheri McGuire
Group Chief Information Security Officer
Standard Chartered Bank
For more information, please contact:

Steve Holt
Ernst & Young LLP (UK)
T: +44 20 7951 7874
E: sholt2@uk.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY is a leader in serving the financial services industry
We understand the importance of asking great questions. It's how you innovate, transform and achieve a better working world. One that benefits our clients, our people and our communities. Finance fuels our lives. No other sector can touch so many people or shape so many futures. That's why globally we employ 26,000 people who focus on financial services and nothing else. Our connected financial services teams are dedicated to providing assurance, tax, transaction and advisory services to the banking and capital markets, insurance, and wealth and asset management sectors. It's our global connectivity and local knowledge that ensures we deliver the insights and quality services to help build trust and confidence in the capital markets and in economies the world over. By connecting people with the right mix of knowledge and insight, we are able to ask great questions. The better the question. The better the answer. The better the world works.

© 2017 EYGM Limited.
All Rights Reserved.

EYG no. 04997-174Gbl
EY-00002836.indd (UK) 08/17.
Artwork by Creative Services Group London.
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

The views of third parties set out in this publication are not necessarily the views of the global EY organization or its member firms. Moreover, they should be seen in the context of the time they were made.

ey.com/fs