Strengthening responses to cyber crime in financial services
Strengthening responses to cyber crime in financial services
From personal identity theft to attacks on national infrastructure, cyber crime is a threat to our society. As US bank robber Willie Sutton Jr., said in 1934, “That’s where the money is,” and this fact makes the financial services industry a prime target.

To highlight this point, in February 2017, Symantec reported that banks and other financial institutions in more than 30 countries were targeted in a spate of attacks, potentially by the Lazarus Group, the organisation credited with the attack on the Bangladesh Central Bank in February 2016.

Lazarus illustrates to us that cyber crime is not only perpetrated by lone hackers taking opportunities where they can, but it is often a business, seeking to maximise value for its stakeholders, either carrying out attacks directly or selling its expertise to third parties.

Faced with an industry which is developing at pace, law and regulations around cyber crime lack the harmonisation and coherence to provide deterrence at scale. Organisations which have been hacked are often punished for failing to meet the required standard of care, and the perpetrators frequently escape justice.

However, because there is no one single legal standard of care, firms that operate across different markets face significant difficulties in building systems and processes that conform to the rules. Finance is a connected and global business and the internet is a borderless tool for attackers. One academic paper even goes so far as to say the current piecemeal local state laws and regulations governing data theft plays directly into the hands of cyber criminals.

Nonetheless, the industry is not helpless and firms can do a lot internally to find solutions to cyber crime. Historically, corporate technology departments have carried the heavy burden of protecting our industry, but this is a business problem. It must move from an IT issue to become an enterprise-wide risk management concern involving all personnel throughout organisations from the board and down. Every employee has an important role to play in protecting their organisation and preventing cyber crime.

Firms need to get the basics right as these are the checks which will help protect organisations against most of the threats. Employees are the first line of defence, and this should be inclusive across all branches of the business at every level.

In particular, governance at organisations must become more comfortable and adept at dealing with cyber risk and information security professionals. Across enterprises, we need to promote a healthy security culture, supported by the right tools, policies and procedures in which we get the basics right to protect our information.

Finally, our approach to cyber team building must adapt, becoming far more diverse, inclusive and multi-disciplinary if we are to remain secure through the onslaught of cyber attacks that we all face.

Margaret Harwood-Jones
Global Head, Securities Services,
Transaction Banking

---

1 “History: Willie Sutton.” FBI. [Online]
Table of contents

Foreword ........................................................................................................... 3
The severity of the cyber threat .......................................................... 5
  Growth in cyber crime
  The cost of cyber crime to business
Who is perpetrating these attacks? ...................................................... 6
  Proliferation of tools and expertise
  The rise of corporate-style hackers
How is cyber crime affecting the financial industry? .......................... 7
  The risk to securities services
  The security risk of new technologies
Regulatory responses to the cyber challenge ..................................... 10
  Regulatory standards governing cyber security
  Global guidance and standards
Internal responses to the cyber threat .................................................. 13
  Getting the basics right in a legacy environment
  Sharing best practices
  Building a security-based culture
  Engaging senior management
  Addressing the talent pool challenge
Conclusions ...................................................................................................... 20
The severity of the cyber threat

Technology advancements have changed the way businesses operate, but they have also ushered in new challenges and threats. Cyber crime is a problem that all organisations are increasingly having to address.

Growth in cyber crime

The Cyber Security Breaches Survey 2016 found that 65% of large UK firms detected a cyber security breach or attack in the previous year. Financial institutions are also being hit by more attacks. Financial institutions reported just five attacks to the Financial Conduct Authority (FCA) during the whole of 2014, but this already stood at 75 in the first nine months of 2016.

Perhaps most alarming is that many firms are unsure if they have had their systems compromised. 36% of respondents to Ernst & Young’s (EY) Global Information Security Survey in 2015 said it was unlikely their organisations would be able to detect a sophisticated attack.

“Cyber breaches are evolving in maturity and it is a very serious systemic risk issue. Businesses are investing heavily in security as a result. Statistics show there are roughly 80% of attacks which are known and that we can protect ourselves against. 15% of attacks are highly complex, and are evolving and difficult to detect. Then there are the 5% of attacks which nobody knows about. It is crucial firms have the ability to react to these threats quickly in the best manner possible,” said Nathalie Lefevre, Cyber Resilience Programme Manager at Euroclear.

The cost of cyber crime to business

Cybersecurity Ventures, a research firm, estimated that global spending on cyber security products and services will exceed USD1 trillion cumulatively between 2017 and 2021.

The costs of these attacks are also increasing. Cybersecurity Ventures added that global annual cyber crime costs will increase from USD3 trillion in 2015 to USD6 trillion by 2021. The report said such costs would be a result of damage and destruction of data; stolen money; lost productivity; theft of intellectual property; theft of personal and financial data; fraud; post-attack disruptions; forensic investigation; restoration and deletion of hacked data; and reputational harm.

Cyber attacks

15% Highly complex attacks that are difficult to detect
5% Unidentified attacks
80% Known attacks

5 Cyber attacks against UK financial industry on the rise – FCA.” Financial Times, 21 September 2016. [Online]
7 Interview with Nathalie Lefevre on 02 June 2017.
Who is perpetrating these attacks?

Threats to organisations are diverse, a point made by the UK’s National Cyber Security Centre, which said attacks are sometimes a result of enterprises opportunistically acquiring technical expertise to execute such crimes, or highly bespoke malware aimed at specific targets.11

Proliferation of tools and expertise

“We have seen an increase in gangs or small criminal cells exchanging cyber attack tools and malware over the dark net. These tools are abundantly available and can be acquired cheaply. Historically, organised criminals viewed cyber attacks as being too hard to perpetrate, but this has changed now that they are able to obtain tools and technical know-how easily and inexpensively. The acumen required to launch cyber attacks today is not that sophisticated,” said Cheri McGuire, Group Chief Information Security Officer at Standard Chartered.12

Historically, organised criminals viewed cyber attacks as being too hard to perpetrate, but this has changed now that they are able to obtain tools and technical know-how easily and inexpensively. The acumen required to launch cyber attacks today is not that sophisticated.

The rise of corporate-style hackers

A growing number of highly professional criminal groups and state-sponsored organisations have been blamed for some of the more damaging attacks. These cyber criminals need to make a return on their investments and are purposely attacking high value targets to maximise their profitability. Many of these groups have been very successful in causing widespread disruption to key infrastructures and industries.

“Companies of criminals are a tier beneath nation state hackers. Think of them as professional companies, which will spend significant amounts of money researching a bank or an enterprise, knowing that the end result will be a lucrative theft. They see such investment as generating a good return. Many of the hackers such as the “lonely heart” scammers, who were initially targeting individuals, have turned into professional cyber criminals and are performing hacks of mid-level organisations regularly,” said Patrick Wheeler, a leading cyber security expert and consultant.13

12 Interview with Cheri McGuire on 26 May 2017.
13 Interview with Patrick Wheeler on 30 May 2017.
How is cyber crime affecting the financial industry?

Cyber criminals have exposed vulnerabilities of financial institutions to disturbing effect.

A systematic hack of Tesco Bank in the UK saw GBP2.5 million stolen from 20,000 accountholders in 2016. Services were also disrupted at Lloyds, Halifax and Bank of Scotland subsequently in January 2017 as a result of a cyber incident.

One of the biggest cyber breaches in history occurred in February 2016, when USD81 million was stolen from the Bangladesh Central Bank by cyber criminals. “Specifically, the attackers exploited cyber weaknesses by designing custom malware tailored to bypass controls and network logging systems used by the Bangladesh Central Bank. The thieves also bypassed fraud controls by using the Bangladesh Central Bank’s credentials to gain unauthorised access to the SWIFT network and by setting up fraudulent bank accounts to receive and transfer the stolen funds,” according to a recent paper by PwC.  

Similar – but less serious hacks – were reported at banks in Ecuador and Vietnam. In response, SWIFT has introduced a number of mandatory and voluntary security measures for its customers. The SWIFT Customer Security Controls Framework has three overarching objectives, namely “Secure your Environment”, “Know and Limit Access” and “Detect and Respond.”


---

14 “SWIFT action: Preventing the next $100 million bank robbery.” PwC, June 2016. [Online]
The risk to securities services

Why is securities services so important?

Securities services is at the heart of the financial services industry providing custody, trade settlement, fund services, issuer services, middle office outsourcing and reporting to major institutional investors, financial institutions and banks and corporates.

The industry safekeeps institutional investor assets globally, and is key in facilitating transactional activities. Financial markets are highly interconnected and interdependent, and a cyber attack would have far-reaching effects for the financial system. It is systemically important and any significant disruption to securities services could have a serious impact on the capital markets.

A cyber breach in the securities services industry could lead to any one of the following adverse scenarios:

**Theft of Assets:** Leading to material losses for the client and custodian.

**Data theft:** Financial institutions trust their custodians with information that is critical and material to their businesses.

**Data corruption and manipulation:** If inaccurate or misleading information is sent to intermediaries or investors, this could result in some of these institutions making erroneous or loss-making decisions based on that information. “The thing that keeps me awake at night is data integrity, and the risk of data manipulation. If asset ownership records were fundamentally changed, then that could undermine confidence in the financial system,” said Nick Seaver, partner at Deloitte’s UK Information and Technology Risk Group.16

**Disruption to clearing and settlement:** “The liquidity condition of financial institutions and their customers depends on the certainty of the assumption that transactions that are considered final will remain final. While erroneous data could result from an extreme cyber event, assurance of the finality of those transactions is necessary to maintain financial stability,” as stated in a paper17 by the Committee on Payments and Market Infrastructures (CPMI).

**Corporate action delays:** These could lead to market uncertainty and prevent end clients from participating in corporate actions.

UCITS V and the Alternative Investment Fund Managers Directive (AIFMD) hold depositaries liable for assets that go missing in custody. The risk of cyber security to asset safety must be prioritised by providers of custody because of this regulatory risk.

---

16 Interview with Nick Seaver on 9 June 2017.

The liquidity condition of financial institutions and their customers depends on the certainty of the assumption that transactions that are considered final will remain final. While erroneous data could result from an extreme cyber event, assurance of the finality of those transactions is necessary to maintain financial stability.

The security risk of new technologies

The securities services industry’s long-term reliance on manual processes is increasingly recognised as impractical and unsustainable. Progress, however, is being made.

Payment instructions in many emerging markets have traditionally been cheque-based, but new technologies such as mobile wallets are changing this in Africa and China. “For example, around half of China’s internet users made payments through their mobile devices last year, and mobile payment transactions more than doubled in 2015 to GBP235 billion,” read a Standard Chartered paper.18 As more transactional activities move online, firms need to increasingly develop and modify their cyber security efforts.

Other disruptive technologies such as blockchain, artificial intelligence (AI) and machine learning are all being scrutinised to see if they will improve efficiencies in securities services. These technologies are being trialled across various processes such as payments, corporate actions and reporting/recordkeeping.

But the industry’s understanding of these disruptors is still limited. This includes understanding of their risks. While the industry is testing these technologies in contained environments, it is crucial the cyber security risks are fully understood before they are rolled out across broader services. “Oftentimes, technological innovations outpace developments in cyber security solutions, standards, and policies, although this can vary across organisations depending on their maturity and size,” added McGuire.

Regulatory responses to the cyber challenge

Regulation of cyber security is not harmonised. Cyber crime is a global threat, and requires an international response.

The challenge here is two-fold: firstly, overly specific regulation can quickly become outdated. Cyber threats are fluid and are becoming increasingly advanced and sophisticated. Some regulators have recognised this, and are reluctant to introduce prescriptive legislation which may become obsolete within a few years or even in a few months’ time.

Secondly, inconsistency in application of rules can cause implementation challenges for global businesses that operate in multiple jurisdictions. If regulation is not harmonised, financial firms will be required to implement different solutions in the different markets in which they operate, causing unnecessary complexity, risks and costs to the industry. Equally, regulatory arbitrage can be harmful, creating potential loopholes or weak spots that can be exploited by cyber criminals.

“International financial institutions may be required to implement bespoke security solutions in individual countries, which may be highly complex and introduce unnecessary risk given the global interconnectedness of their technology platforms. More needs to be done to harmonise global cyber security regulations,” said McGuire.

Prescriptive regulation also puts the authorities at risk of not being forward-thinking enough. “Prescriptive regulation will solve yesterday’s problem, but it will not solve tomorrow’s problem,” said Seaver.

Regulatory standards governing cyber security

Policymakers are seeking to address the growing threat of cyber attacks. The European Union (EU) for instance, passed legislation to increase national and critical infrastructure capabilities to combat cyber crime through the Network Information Security (NIS) Directive, which will come into effect in 2018. It applies to what policymakers refer to as “operators of essential services,” and the financial services sector is one of them. It obliges organisations to implement measures to reduce cyber risk and report incidents to the relevant authorities.  

The NIS Directive outlines that organisations must reduce cyber risk by having appropriate corporate governance and compliance procedures; secure and regular monitoring of technology systems and networks; employee training in cyber risks; and the maintenance of a functioning business continuity plan (BCP). These rules complement the General Data Protection Regulation (GDPR), which will require financial institutions (among other industries) to take a range of steps to assure privacy of employee and customer data, as well as disclose data breaches to the relevant authorities.

As such, the EU is broadly consistent in its approach towards cyber security, although there is usually a small amount of variation in terms of rule implementation across member states.

Inconsistency of cyber security rules is a global phenomenon. Standards and expectations about cyber protections and disclosure rules around breaches are not aligned. Executives surveyed by The Economist Intelligence Unit felt cyber security received insufficient political attention. 77% of executives said politicians did not take seriously the systemic risk of cyber security, namely the ability of criminals to shut down physical and financial infrastructure.
In Asia-Pacific, cyber security and data protection regulations are highly fragmented. According to a Jones Day report, China introduced cyber security laws in 2017, which subject industries including financial services to a number of requirements. These include security compliance obligations such as network inspections, staff education, background checks on personnel, and the implementation of a disaster recovery plan. The report added that data generated in China must be held locally and security reviews must be conducted if information is transferred outside of the country.22

Other markets have a less developed approach to cyber crime. Vietnam introduced the Law on Cyber Information Security in 2016, and there is confusion as to what constitutes compliance.23 Asia is particularly prone to cyber-attacks with a Marsh & McLennan Companies report stating hackers were 80% more likely to attack organisations in Asia, while these companies took 1.7 times longer than the global median to discover a breach.24

If countries pose a heightened cyber security risk, then organisations simply will not invest in them. The Economist Intelligence Unit study found cyber security risk was a top five reason among 31% of executives for not investing in an otherwise promising country. Cyber security risk was also a top five reason among 19% of executives for reducing operations in a region.25

Piecemeal regulation will not beat cyber crime. The adoption of standards and best market practices will, however, provide regulators with a benchmark for which to work from. Law enforcement and the legal framework for cyber crime is not as mature as rules around drug trafficking, for example. Consistent global standards and best practices need to be buttressed by robust and effective enforcement frameworks.

Global guidance and standards

Global standards, though not necessarily required by regulation, are a good foundation for organisations to base their cyber security programmes on. “There are several standards around cyber-best practices including the ISO 27000 series and those outlined by the National Institute of Standards and Technology (NIST),” commented Wheeler.

Most financial institutions appear to be adopting NIST, added Seaver. “There are a number of different standards, which all heavily overlap each other. NIST is good in the sense that it focuses not just on cyber defence but also on recovery,” he said.

CPMI-IOSCO (International Organisation of Securities Commissions) has also provided guidance to financial market infrastructures (FMIs) on cyber security. Its report – “Guidance for Cyber Resilience for FMIs – June 2016”26 – stated the following were essential for firms to ensure they had robust cyber security protocols:

- Sound cyber governance. Board and senior management are critical to a successful cyber resilience strategy.
- The ability to resume operations quickly and safely after a successful cyber attack is paramount.
- FMIs should make use of good quality threat intelligence and rigorous testing.
- FMIs should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience at every level within the organisation.
- Cyber resilience cannot be achieved by an FMI alone; it is a collective endeavour of the whole ecosystem.27

Financial institutions, particularly those offering securities services, need to have ongoing and open channels of communication with regulators, advising them on how to approach these threats and, to provide feedback where applicable. At the same time, public policy, compliance and in-house legal teams need to continually engage with the broader business about their obligations.

---

Getting the basics right is key, although this can be a challenge for large organisations with legacy technology requiring regular updates.
Internal responses to the cyber threat

Alongside the development of external regulations and standards to improve cyber security, the industry itself can do much to improve the situation.

Getting the basics right in a legacy environment

“Getting the basics right is key, although this can be a challenge for large organisations with legacy technology requiring regular updates. Having strong cyber security practices and governance in a globally connected business requires strong management and leadership from the top,” said McGuire.

Many organisations will already be focused on:

- Up-to-date firewalls and regular anti-virus checks
- Password protection
- Encrypted email and communications
- Segregation between personal and work devices
- Limits on social media and personal email on work devices
- Prohibition on using public Wi-Fi
- Permissioned access to sensitive data or information
- Banning USBs or portable storage devices

Nevertheless, experts acknowledge there is still more to do in terms of education and developing a risk culture across organisations. In a recent webinar on cyber security in financial services, delegates called for more punitive sanctions against staff who regularly breach data security rules, in the same way as firms would deal with other serious conduct issues.

Sharing best practices

Industries can protect themselves from cyber criminals by engaging with each other, and sharing best practices and ideas within a trusted group. Collaboration between financial institutions has been underway for many years to share information on attack vectors and helping to prevent cyber attacks.

The Cyber Defence Alliance – of which Standard Chartered is an active member – was established in 2015 by several major European banks to exchange information about cyber threats. The initiative has close links with law enforcement divisions such as the City of London Police and the UK National Cyber Crime Unit. Other collaborative groups include the Financial Services Information Sharing and Analysis Center (FS-ISAC), which was established in 1999 and has a global membership. Industry-wide cooperation is essential to ward off cyber threats.

7 habits of a highly secure organisation

- Current software versions
- Up-to-date anti-malware protection
- Engaged senior management
- Diverse security teams
- Multi-disciplinary approach
- Educated staff
- Relentless testing

Source: Kaspersky Lab UK

“Collaboration is increasing and our business has a lot of contact and conversations with external companies, discussing new threats and challenges in cyber security,” said the market infrastructure Group Information Security Officer.

**Building a security-based culture**

Sharing information across the industry is clearly useful, but vigilance must begin within one’s own organisation. Managers need to ensure their staff understand cyber security risks. This requires leadership and cultural change. Meeting the minimum standards on cyber security is not enough.

Firm-wide education needs to be promoted as cyber risk is not exclusive to any particular branch of a business. Such exercises should not be ad hoc or simply reactive to a crisis, but continuous and regular. Employees should be warned about the implications a cyber security event could have on clients, brand reputation, and share value. Staff education on cyber security risks such as phishing and malware needs to be undertaken and this guidance should be documented, updated and readily available for reference.

Physical security is also important. A breach could occur if the custodian’s premises are broken into and access is gained to the system. The physical environment can also be jeopardised by criminals gaining employment at the custodian and obtaining “legal” access to the systems and potentially, positions of trust.

“Standard Chartered fosters a culture of security awareness across the globe at all of our sites and uses an array of approaches for our awareness programme, beyond mandatory annual computer-based training. For example, we have designated ‘security champions’ at sites and hold regular security seminars, and we also perform simulation exercises. This may involve simulated phishing tests of our employees and conducting quantitative analysis off the back of it to assess how effective our training and awareness programmes have been. Cyber security should not be viewed solely as an IT or technology issue. All of our staff can and must play a role in mitigating the risks,” said McGuire.

**Engaging senior management**

A firm-wide approach to cyber security awareness and compliance needs to be defined by the C-suite executives and board directors at organisations. The recent cyber attacks pose an existential threat to businesses in general, and financial institutions in particular. And clearly, more work needs to be done in this area. While the Economist Intelligence Unit study indicated that cyber security functions were increasingly on the agenda among C-suite executives, a paper by Accenture found two-thirds of banking executives did not believe their business unit and cyber security strategies were aligned with the leadership and across the organisation.

Such disconnects need to be addressed quickly at banks. Put simply, governance must be aligned

with the new threats, and this means banks need to invest greater focus on their cyber security strategic approaches at the most senior levels. While banks recognise that they are not immune to all threats, and thus must make preparations on how they deal with potential breaches, many board-level executives are not comfortable enough with the subject to set direction. The structure at the top needs alignment on cyber security risks and strategies, for them to permeate down through the organisation and its culture as a whole.

Addressing the talent pool challenge

Organisations themselves also need a mindset shift. They have to start viewing cyber crime risk as business-critical, and allocate the appropriate resources and focus to build the right approaches, strategies, policies and skill sets.

The challenge however, is that there is a cyber security talent pool shortage. Cybersecurity Ventures said there were an estimated one million cyber job openings in 2016, pointing out that 209,000 cyber roles lay unfilled in the US.31 “The cyber security industry is at negative employment and global leaders in the US, UK, India and other nations have talked about the shortages of expertise in this domain. If institutions want to be able to protect and defend their infrastructure, they need to find the right talent. This is a priority agenda item for many CEOs and government leaders,” commented McGuire.

The market infrastructure Group Information Security Officer agreed. “There are a lack of experts in the cyber security industry, and this is a problem. As attacks become more sophisticated with new features, the industry needs to have expertise in order to handle such problems,” she said.

But how can this be achieved? Ultimately, these skills need to be acquired at a younger age, even before university and high school. It is true that a number of STEM (science, technology, engineering and mathematics) schools have proliferated and are doing remarkable work, but education about cyber security needs to begin far earlier. Educating young people about cyber issues must become a long-term objective for governments and educational institutions.

“Children nowadays – even in their strollers – are using devices such as iPads so it is even more important that security and privacy lessons are taught at an early age in the schools and incorporated into the curriculum. Furthermore, we are seeing increasing numbers of middle and high schools teach code, but we also need to introduce more training programmes and internships for young people,” said McGuire.

This instruction obviously needs to be accentuated at higher levels of education and graduate training too. “Standard Chartered, for example, has partnered with a number of leading universities across Asia, and brought graduates into its Group Information Security team. It is also important to attract talent from multidisciplinary areas, in addition to those with deep technical expertise, because cyber security is a business-wide problem. Drawing talent from a diverse pool helps bring a more well-rounded approach to critical thinking and problem solving,” she added.

Others believe the lack of diversity in the cyber security industry needs to be resolved, as women have limited representation in cyber security roles globally.

Drawing talent from a diverse pool helps bring a more well-rounded approach to critical thinking and problem solving.
Strengthening responses to cyber crime in financial services

Male and female cyber security workforce composition, by region

In terms of seniority, very few women reach the most senior cyber positions in any geographical region.

Gender distribution by organisational position of the cyber security workforce, by region

<table>
<thead>
<tr>
<th>C-level executive</th>
<th>North America</th>
<th>Latin America</th>
<th>Europe</th>
<th>Africa</th>
<th>Middle East</th>
<th>Asia-Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Men</td>
<td>99%</td>
<td>100%</td>
<td>100%</td>
<td>99%</td>
<td>99%</td>
<td>99%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Executive management</th>
<th>North America</th>
<th>Latin America</th>
<th>Europe</th>
<th>Africa</th>
<th>Middle East</th>
<th>Asia-Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Men</td>
<td>99%</td>
<td>100%</td>
<td>100%</td>
<td>99%</td>
<td>99%</td>
<td>99%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Director/Middle management</th>
<th>North America</th>
<th>Latin America</th>
<th>Europe</th>
<th>Africa</th>
<th>Middle East</th>
<th>Asia-Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women</td>
<td>2%</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>Men</td>
<td>98%</td>
<td>99%</td>
<td>99%</td>
<td>99%</td>
<td>100%</td>
<td>99%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Manager</th>
<th>North America</th>
<th>Latin America</th>
<th>Europe</th>
<th>Africa</th>
<th>Middle East</th>
<th>Asia-Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women</td>
<td>17%</td>
<td>28%</td>
<td>23%</td>
<td>35%</td>
<td>34%</td>
<td>40%</td>
</tr>
<tr>
<td>Men</td>
<td>83%</td>
<td>72%</td>
<td>77%</td>
<td>65%</td>
<td>66%</td>
<td>60%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-managerial staff</th>
<th>North America</th>
<th>Latin America</th>
<th>Europe</th>
<th>Africa</th>
<th>Middle East</th>
<th>Asia-Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>Men</td>
<td>99%</td>
<td>99%</td>
<td>99%</td>
<td>100%</td>
<td>100%</td>
<td>99%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Entry level</th>
<th>North America</th>
<th>Latin America</th>
<th>Europe</th>
<th>Africa</th>
<th>Middle East</th>
<th>Asia-Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
<td>1%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Men</td>
<td>100%</td>
<td>99%</td>
<td>100%</td>
<td>99%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contractor</th>
<th>North America</th>
<th>Latin America</th>
<th>Europe</th>
<th>Africa</th>
<th>Middle East</th>
<th>Asia-Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women</td>
<td>8%</td>
<td>5%</td>
<td>8%</td>
<td>4%</td>
<td>4%</td>
<td>4%</td>
</tr>
<tr>
<td>Men</td>
<td>92%</td>
<td>95%</td>
<td>92%</td>
<td>96%</td>
<td>96%</td>
<td>96%</td>
</tr>
</tbody>
</table>
The absence of gender diversity in cyber roles is a problem as it makes it harder to recruit talented, younger or millennial women to those roles. PwC analysis shows that an employer’s policy on diversity, equality and workforce inclusion is very important to millennials.32

### Millennials and diversity

**How important is an employer’s policy on diversity, equality and workforce inclusion when you decide whether or not you should work for them?**

<table>
<thead>
<tr>
<th></th>
<th>Female</th>
<th>Male</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important</td>
<td>82%</td>
<td>74%</td>
</tr>
<tr>
<td>Neither</td>
<td>12%</td>
<td>15%</td>
</tr>
<tr>
<td>Not important</td>
<td>6%</td>
<td>11%</td>
</tr>
</tbody>
</table>

Source: PwC Millennials at work research

The onus is therefore on organisations to change attitudes and workplace practices.

Encouraging more flexible working conditions is one of the ways employers such as Standard Chartered are promoting workforce and gender diversity. Standard Chartered is doing this through implementing a global policy on flexible working with simpler administrative procedures. Standard Chartered is also rolling out increased minimum paid parental leave of 20 weeks for the mother and two weeks for the spouse or civil partner on a global basis.

Standard Chartered has signed up to the Women in Finance Charter, which will set internal targets on gender diversity in senior management. The pay of the senior executive team will be linked to the delivery of these targets. In addition, Standard Chartered set up a Global Women’s Network, which helps provide support and encouragement to female colleagues. Research often shows diverse teams are high performing and this clearly applies to cyber security.

“Diversity is a must – not just in cyber – but in all domains. If you want to be successful in business, do not recruit people similar to yourself. It is critical to build on talent and look for individuals with complementary skills,” commented Lefevre.

Cognitive diversity is also key, and will enable cyber security experts to engage better with board directors and senior managers, and this will ultimately help organisations deal with these new challenges holistically. It is imperative that further work be done to encourage women to contemplate working in the burgeoning cyber security industry.

Wheeler also emphasised the number of women employed in cyber security is very low, but highlighted the argument was more nuanced than just simply hiring more female staff. “The cyber realm is usually occupied by males over a certain age with a similar technical preparatory background. There is a low realm of diversity and with it, cognitive diversity. But hiring more women with the same background as those males is not necessarily going to change things. It is critical not only more women – but also ethnic minorities and persons with different skill sets and personal backgrounds – are introduced into the world of cyber to grow our cognitive diversity,” he said.

Identifying quality female candidates with non-technology backgrounds will help widen the talent pool available. “Nearly all of the senior people I know working in cyber security stumbled into their roles, and they all had different backgrounds. The challenge for the industry is engineering these ‘happy accidents’ on an industrial scale,” added Wheeler.

Efforts are already in train to encourage more women to take up cyber security roles in the industry.

For example, Euroclear’s IT business units are actively involved in such schemes, said Katrien Goosens, HR Global Diversity & well-being officer. “Euroclear is working with non-governmental organisations (NGOs) such as Greenlight for Girls which hold events for young girls aged between six and 12 to get them excited about STEM subjects. We believe it is important to widen the talent pool, particularly because there is a scarcity of cyber-security experts. Other organisations are setting up career clinics for women looking for new opportunities or careers in cyber-security,” said Goosens.33

---

33 Interview with Katrien Goosens on 02 June 2017.
Case Study 1: Standard Chartered and Goal

Goal is a Standard Chartered initiative active in 20 countries designed to empower and equip adolescent girls with the confidence, knowledge and skills they need to be integral economic leaders in their families, communities and societies. In 2017, the bank will add another 80,000 young ladies to the programme, bringing the total over its 11-year lifespan to 365,000. Quite remarkable considering that it started with only 70 girls in Delhi, India.

The curriculum is based on four training modules. “Be Money Savvy” focuses on financial education. “Be Yourself” imparts communication skills. “Be Healthy” builds knowledge on health and hygiene and “Be Empowered” teaches girls confidence and life skills. The programme is being continually improved. Modules around English language training and digital literacy to help develop young women’s computer aptitude, word processing and web mobility skills are being launched.

Initiatives like these will help accentuate women in the workplace in emerging markets. By expanding the scheme to digital skills and literacy, it is hoped more women will move into the IT universe, including cyber security.

Case Study 2: The CyberWayFinder

The CyberWayFinder initiative was set up by cyber security experts to enable more women of all ages to succeed in cyber security as a career option to redress the talent shortfall. The initiative works primarily out of Belgium, with candidates drawn out of Benelux markets. The scheme hopes to expand further into Hong Kong, Kuala Lumpur, London and Paris.

The three-year work/learn programme provides jobs in cyber security while teaching a number of core disciplines from problem solving to coding and operations. It helps women transition in and attain professional qualifications as well as work experience with a brand name employer. In addition, it is not just aimed at young female graduates, but those in mid-career or older. Early results indicate that 100% of candidates on the programme have found work in the industry, reflecting the acute talent shortage that firms are facing.
Conclusions

Cyber threats are becoming more frequent and sophisticated. A serious hack could destabilise a systemically important financial institution. Banks – including those offering securities services – must be prepared to deal with this challenge.

Regulation of cyber security is neither globally unified nor standardised, and this presents challenges for organisations with global footprints. Financial institutions should implement international standards and cyber security best practices. Maintaining basic cyber hygiene is key to preventing cyber security incidents.

Collaboration and business-wide education at financial institutions about cyber security is key. There needs to be a cultural change that embeds cyber security as every employee’s responsibility, supported by the right tools, policies and procedures, and implemented top-down.

Cyber security talent is in short supply and organisations need to expand the pools from which they hire. Having a diverse team with different backgrounds can help drive cognitive diversity, and this will be critical in the fight against cyber crime.

It is imperative that further work be done to encourage and attract women to working in the cyber security industry.

Responsible organisations like Standard Chartered have established programmes to empower the next generation of women in the workplace, which in the long term will deepen the talent pool, and help bring different perspectives and approaches to the table.
Margaret Harwood-Jones
Global Head, Securities Services, Transaction Banking

Margaret Harwood-Jones is Global Head, Securities Services for Transaction Banking at Standard Chartered Bank.

Based in Singapore, Margaret joined the Bank in January 2013. Her initial responsibility was leading the business agenda for Financial Intermediates and Institutional Investor clients on a worldwide basis, across cash management, securities services and trade finance. Her primary mandate was to drive growth and to take the business performance to the next level in its development.

In August 2016 Margaret was appointed to her current role. Her responsibility is to provide strategic leadership for the Securities Services business globally, leading and co-ordinating the activities of all functions which comprise the business unit (Operations, Technology, Client Management, Business Development and Product Management). She represents the business both across the wider bank and in the external market. Her former duty remains in place within this broader remit.

Margaret has more than three decades of experience in financial services, almost 20 years of which has been within the securities services industry. Previously in senior manager positions at BNP Paribas, and before that at HSBC, Margaret has undertaken roles in global sales management, relationship and service management, marketing, strategic development and business unit leadership for global custody and corporate trustee activity.

Margaret is a Chartered Individual of the Securities and Investment Institute and an Associate of the Institute of Bankers. She was a founding Executive Director of the Depository and Trustee Association in the UK. Margaret holds a General Management Programme certificate granted by the European Centre for Continuing Education, INSEAD, France.
Notes
Committing our expertise to power your ambition

Local service on a global scale
With a presence in 68 countries and a unique footprint covering Asia, Africa and the Middle East, Standard Chartered’s business combines global capabilities with deep local knowledge to provide innovative products and services to meet the diverse and ever-changing needs of our corporate and institutional clients in the world’s most dynamic markets.

Your partner for the long run
Building on a rich banking heritage of over 160 years, Standard Chartered is committed to providing a working partnership that builds your business with value-added and strategic solutions that reflect our longevity and unparalleled success. We are committed to our clients, employees and communities at all times.

Dedicated to sustainable success
As a leading international bank, our success is built on teamwork, partnership and the diversity of our people. With a long-term strategy to build a sustainable business, Standard Chartered leads by example in helping to develop emerging markets and ensuring we make a positive impact on society and the environment.

The right capabilities for your needs

<table>
<thead>
<tr>
<th>Transaction Banking</th>
<th>Corporate Finance</th>
<th>Digital Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Markets</td>
<td>Principal Finance</td>
<td>Global Research</td>
</tr>
</tbody>
</table>

Angola  Argentina  Australia  Bahamas  Bahrain  Bangladesh  Botswana  Brazil  Brunei  Cambodia  Cameroon  Canada  Chile  China  Colombia  Cote d’Ivoire  Egypt  Falkland Islands  France  Gabon  Germany  Ghana  Guernsey  Hong Kong  India  Indonesia  Iraq  Ireland  Italy  Japan  Jersey  Jordan  Kenya  Laos  Lebanon  Luxembourg  Macau  Malaysia  Mauritius  Mexico  Mongolia  Myanmar  Nepal  Nigeria  Oman  Pakistan  Peru  Philippines  Qatar  Saudi Arabia  Sierra Leone  Singapore  South Africa  South Korea  Sri Lanka  Sweden  Switzerland  Taiwan  Tanzania  Thailand  Turkey  Uganda  United Arab Emirates  United Kingdom  United States of America  Vietnam  Zambia  Zimbabwe