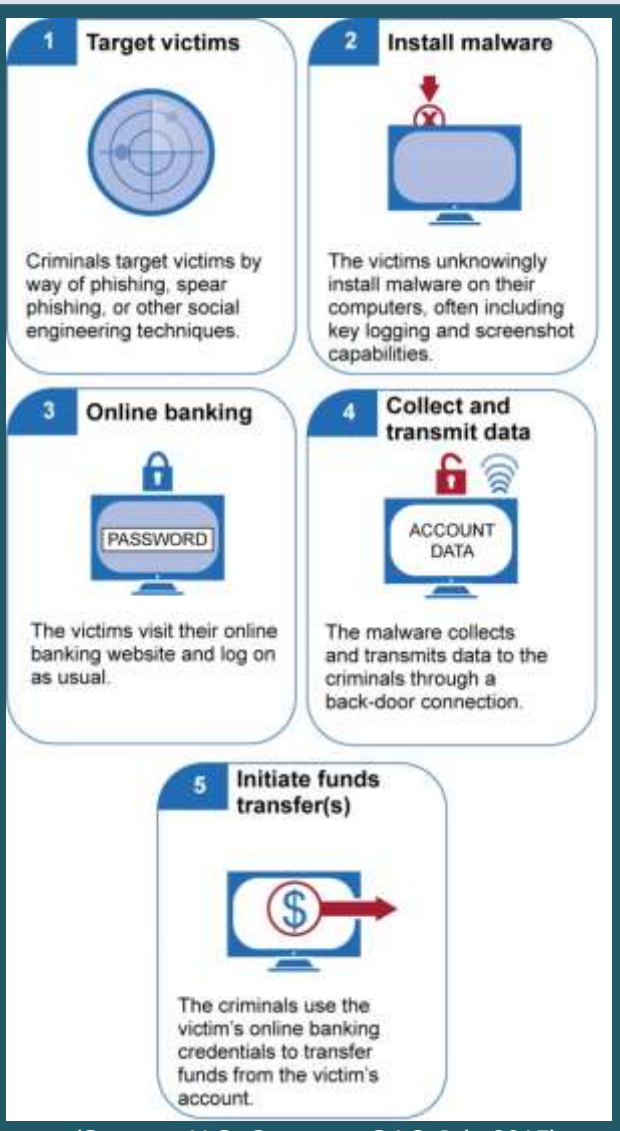
2015

Banking, Financial Services, Retail & Payment Services Cyber-Crime



(**Source:** U.S. Congress GAO July 2015)

Homeland Security Research Corp.

Banking, Financial Services, Retail & Payment Services Cyber-Crime – 2015

August 2015

Homeland Security Research Corp. (HSRC) *is an international market and technology research firm specializing in the Homeland Security (HLS) & Public Safety (PS) Industry. HSRC provides premium market reports on present and emerging technologies and industry expertise, enabling global clients to gain time-critical insight into business opportunities. HSRC's clients include U.S. Congress, DHS, U.S. Army, U.S. Navy, NATO, DOD, DOT, GAO, and EU, among others; as well as HLS & PS government agencies in Japan, Korea, Taiwan, Israel, Canada, UK, Germany, Australia, Sweden, Finland, Singapore. With over 750 private sector clients (72% repeat customers), including major defense and security contractors, and Fortune 500 companies. HSRC earned the reputation as the industry's Gold Standard for HLS & PS market reports.*

Washington D.C. 20004, 601 Pennsylvania Ave., NW Suite 900,
Tel: 202-455-0966, info@hsrc.biz, www.homelandsecurityresearch.com

Table of Contents

List of Tables

List of Figures

1 Banking, Financial Services, Retail & Payment Services Trojans

(**Source**: Cisco)

- Today's financial services Trojans typically utilize an updatable and encrypted configuration file which is stored in the file system, the registry or is actually embedded in the Trojan itself. Types of institutions being targeted by Trojans:

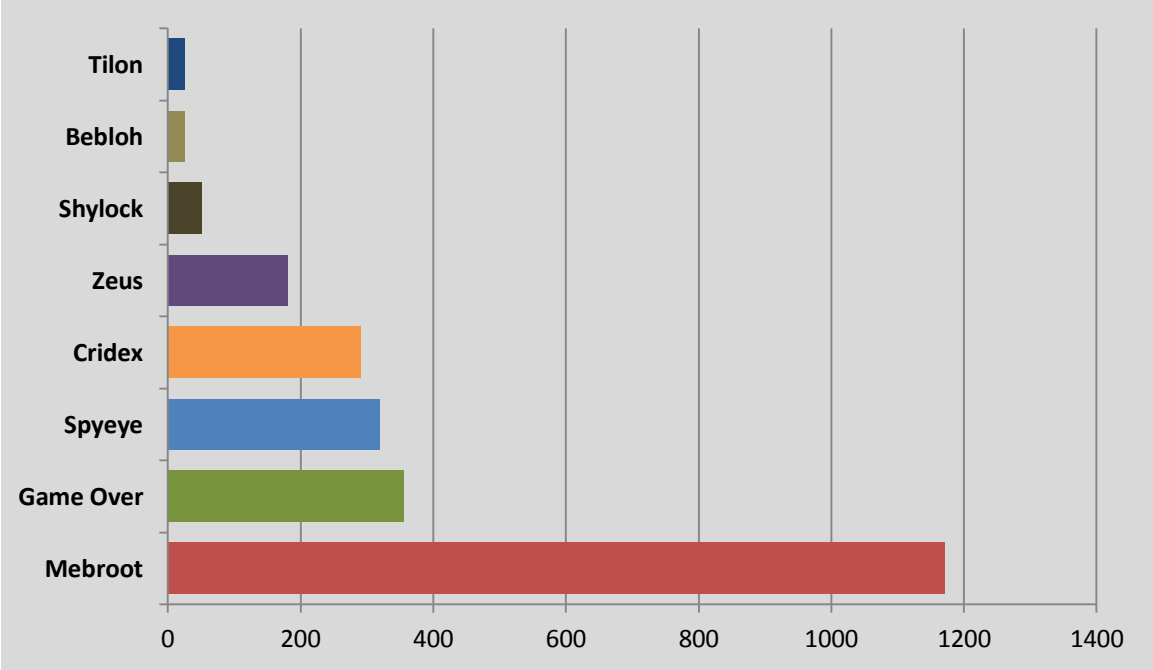
"In the financial sector more than 16% of IT budget is spent on average on Cyber-security"

- Nearly every sector of financial institution is targeted, from commercial banks to credit unions. Traditional banking websites were the focus of most of the campaigns, but attackers are also exploring different institutions that facilitate online transactions. Institutions that facilitate high volume, high value transactions, such as Automated Clearing Houses (ACH), have been targeted, as well as platforms shared by a number of banks and even payroll systems.

"Financial institutions have been fighting malware that targets online banking for over ten years".

- Attackers prefer to target institutions in developed countries with sizeable populations and wealthy residents. This makes sense as there is a large potential base of individuals to compromise with a high potential return. Different global factors can influence attackers' decisions, such as spoken languages and countries where international transactions are more difficult and require local steps to launder the money.

Figure 1 - Number of Institutions Targeted by Each Trojan



(**Source**: Cisco, HSRC)

1.1 Cybercrime Risk Assessment

- Although cyber attackers are aggressive and likely to relentlessly pursue their objectives, financial services companies are not passive victims. The business and technology innovations that financial services companies are adopting in their quest for growth, innovation, and cost optimization are in turn presenting heightened levels of cyber risks. These innovations have likely introduced new vulnerabilities and complexities into the financial services technology ecosystem.
- For example, the continued adoption of Web, mobile, cloud, and social media technologies has likely increased opportunities for attackers. Similarly, the waves of outsourcing, offshoring, and third-party contracting driven by a cost reduction objective may have further diluted institutional control over IT systems and access points. These trends have resulted in the development of an increasingly boundary-less ecosystem within which financial services companies operate, and thus a much broader "attack surface" for the threat actors to exploit.
- Complicating the issue further is that cyber threats are fundamentally asymmetrical risks, in the sense that often times, small groups of highly skilled individuals with a wide variety of motivations and goals have the potential to exact disproportionately large amounts of damage.

- Yesterday's cyber-risk management focus on financial crime was and still is essential. However, in discussions with clients, it appears that they are now targets of not only financial criminals and skilled hackers, but also increasingly of larger, well-organized threat actors, such as hacktivist groups driven by political or social agendas and nation-states, to create systemic havoc in the markets.
- An illustrative cyber threat landscape for the banking sector suggests the need for financial services firms to consider a wide range of actors and motives when designing a cyber-risk strategy. This requires a fundamentally new approach to the cyber-risk appetite and the corresponding risk-control environment.
- The combination of secured Storage Server, like Cisco "Red HAT' UCS big data servers and Splunk Enterprise represents a robust technology combination. Deploying these technologies together not only provides for expandable cost-effective storage, but it can expand the analysis that can be done on machine data while extending retention times. Together, these strengths can help Banking, Financial Services, Retail & Payment Services organizations reduce the risk, cost and complexity of building a world class cybersecurity analytics platform

"Striking a balance between security and accessibility is key to a successful cybersecurity approach."

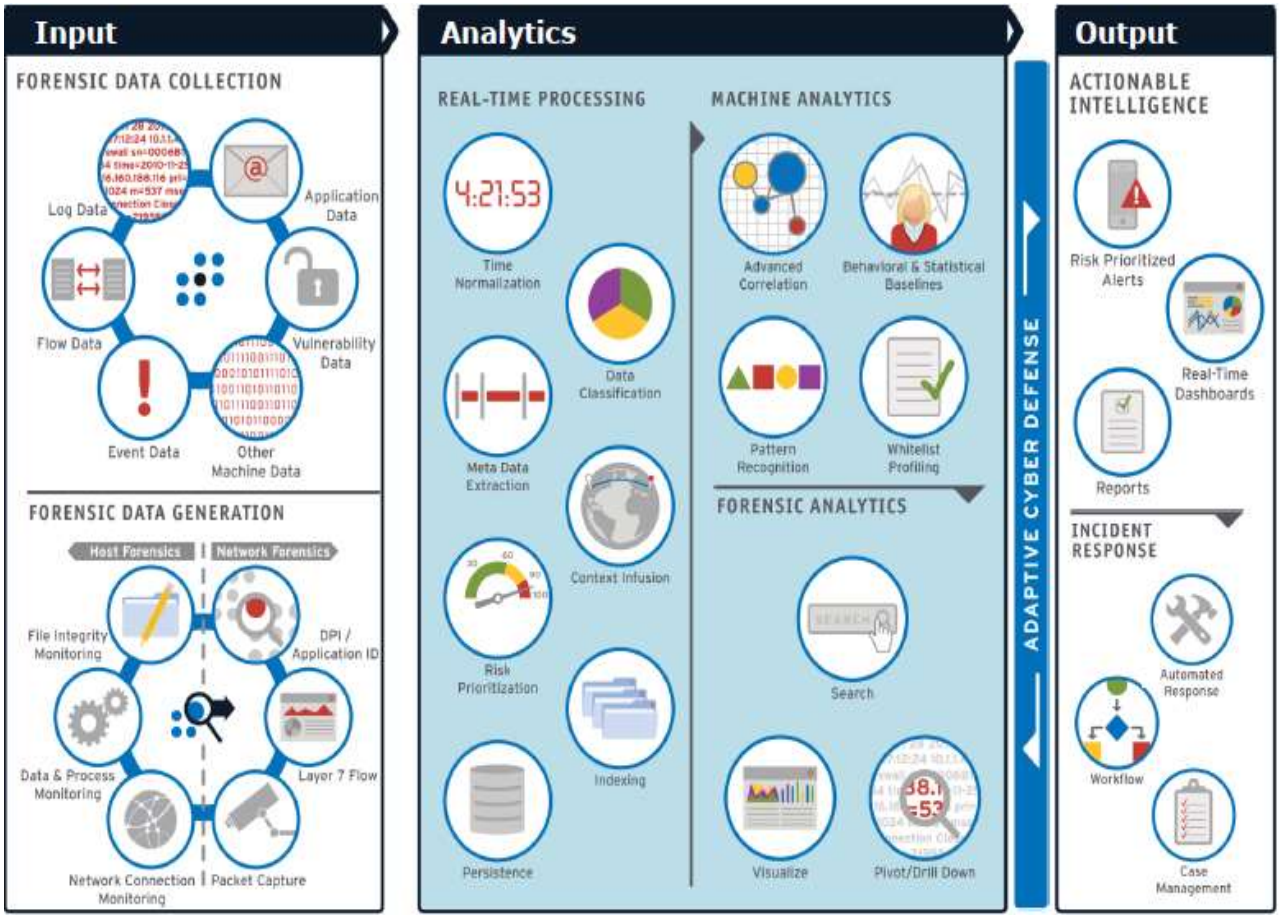
- Criminal activities in cyberspace are increasingly facilitated by burgeoning black markets for both tools (e.g., exploit kits) and take (e.g., password information). Understanding the current and forecasted outlook for these grey-black markets lays the groundwork for follow-on exploration of options to minimize the potentially harmful influence these markets impart. The period of this report and further beyond will bring more activity in darknets, more use of crypto-currencies (e.g. Bitcoin), greater anonymity capabilities in malware, and more attention to encrypting and protecting communications and transactions; that the ability to stage cyberattacks will likely outpace the ability to defend against them; that crime will increasingly have a networked or cyber component, creating a wider range of opportunities for black markets; and that there will be more hacking for hire as-a-service offerings, and brokers.
- There is a debate in the cybersecurity community on who will be most affected by the expanding black market (e.g., small, medium or large businesses, individuals), what products will be on the rise (e.g., fungible goods, such as data records and credit card information; non-fungible

goods, such as I.P.), or which types of attacks will be most prevalent (e.g., persistent, targeted attacks; opportunistic, mass "smash-and-grab" attacks)

1.2 Cybercrime, the Banking, Financial Services, Retail & Payment Services Perspective

- The sector deals with some of the most highly valuable assets, from people's money and their personal information to highly sensitive and proprietary algorithms. This makes Banking, Financial Services, Retail & Payment Services firms particularly susceptible to cyber threats.
- Recognizing the gravity of the situation, regulators have made it a priority to address cybersecurity issues, such as taking proactive strides to adopt government standards for reporting breaches and creating cybersecurity standards in the private sector. Still, there are concerns that heavier regulation in the banking & financial services industry may not be optimal.
- Recent data breaches at large national retailers have underscored the difficulty of securing customers' financial data and the vulnerability of retail point-of-sale terminals, which are a prime target for cyber thieves.

Figure 2 - A Financial Service Enterprise Cybersecurity Platform



(**Source**: J. Zulberg LogRhythm)

- 80% of senior managers think that a cyber-attack is more dangerous to their country than a physical attack. Additionally, 51% believe that a cyber-attacker is present right now in the IT network of their organization, or that he had a presence in the organizational network during 2014.
- The data is based on interviews with 989 managers at the level of President/Vice-president and with IT managers from over the entirety of the United States, Canada, Europe and Asia Pacific.
- In 2013, Trojans were targeted at over 1,400 financial institutions worldwide and compromised millions of computers.

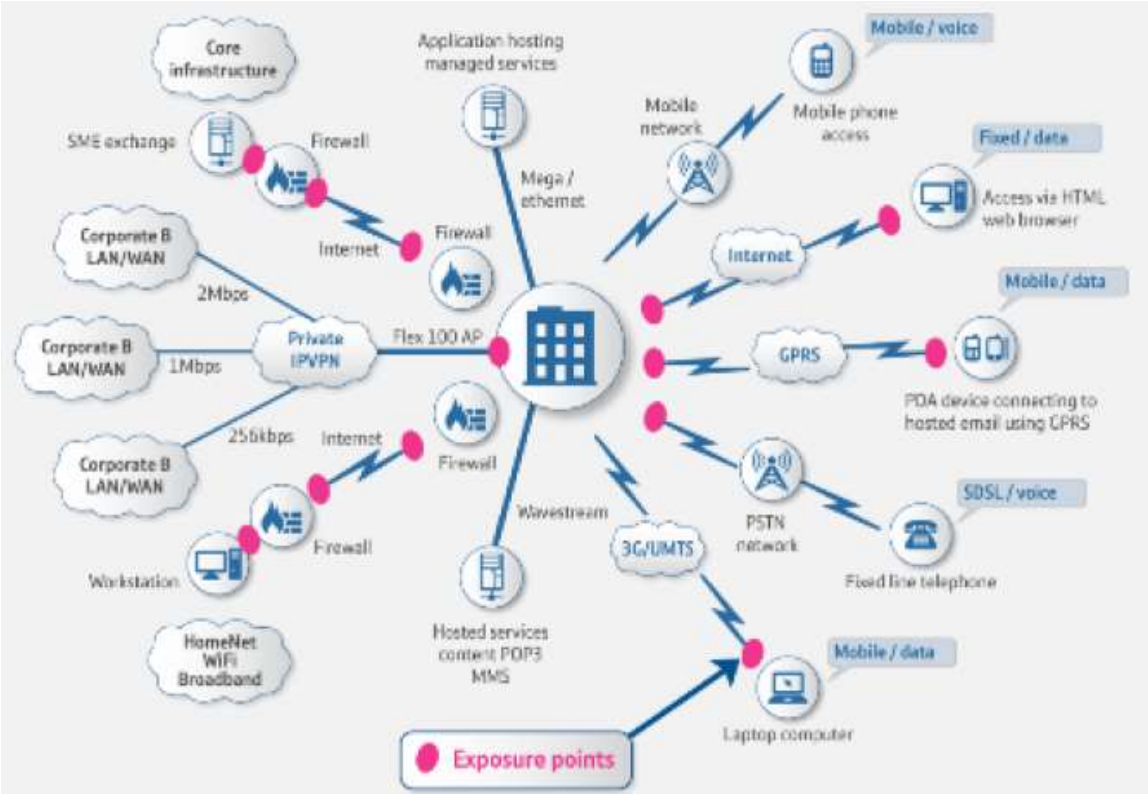
"Without audits and monitoring, security teams will face an uphill battle when they attempt to manage the state of controls, policies and events over time"

When targeting these institutions, many attackers opt for either a focused attack or a broad strokes approach.

(**Source**: Cisco)

- The survey shows a steep rise in the industry managers` awareness of threats from cyber attackers. Among the reasons for the rise in awareness are repeated reports on cyber-attacks by countries on critical infrastructures and business organizations, combined with reports on intruding into the most sensitive information assets, such as the latest NSA affair.
- The most costly cybercrimes are those caused by denial of service
- By September 2014, a team of researchers, at the University of California, have identified a weakness believed to exist in Android, Windows and iOS mobile operating systems that could be used to obtain personal information from unsuspecting banking & financial services users. They demonstrated the hack in an Android phone. Among the apps they easily hacked were Gmail, CHASE Bank and H&R. Block online tax filing and tax software with a 48% success rate, was the only app they tested that was difficult to penetrate. The researchers monitor changes in shared memory and are able to correlate changes to what they call an "activity transition event," which includes such things as a user logging into Gmail or H&R Block or a user taking a picture of a check so it can be deposited online, without going to a physical CHASE Bank. Augmented with a few other side channels, the authors show that it is possible to fairly accurately track in real time which activity a victim's app is in.
- Mitigation of such attacks requires enabling technologies such as SIEM, intrusion prevention systems, application security testing and enterprise governance, risk management and compliance (GRC) solutions.

Figure 3 - Cloud, Convergence, Consolidation & Mobility Infrastructure of a Bank



(**Source**: L. Beeson)

- Increasingly, banking institutions are reluctant to acknowledge and much less discuss the ongoing distributed-denial-of-service, malicious insiders and web-based attacks against their services. Perhaps that's because they're concerned that consumers will panic or that revealing too much about the attacks could give hacktivists information they could use to enhance their abilities.
- In recent regulatory statements, some banks are candid about DDoS attacks and their impact. In their annual 10-K earnings reports, filed with the Securities and Exchange Commission, seven of the U.S. top 10 Banking, Financial Services, Retail & Payment Services institutions provided details about the DDoS attacks they suffered.
- Within the broad Banking, Financial Services, Retail & Payment Services IT market, there are four major but inter-dependent trends that are reshaping the capabilities of technology and also restructuring the fundamental market dynamics of the industry. These trends are:
  - Cloud computing
  - Mobility

- Social computing
- Big data & analytics.

❑ These four key trends are driving growth in the Banking, Financial Services, Retail & Payment Services IT sector, and their relationship with banking & financial services cybersecurity is fundamental. Each of these trends both impacts and is impacted by cybersecurity and that impact can be either positive or negative. Cybersecurity then, is tied intrinsically to the shape of the overall banking & financial services IT market.

Table 1 - The Banking, Financial Services, Retail & Payment Services ICT Environmental Change Factors

Cloud, convergence, consolidation and mobility
•Infrastructure complexity and criticality increasing **•Mobile devices are now a reality** **•It is not obvious where your assets are or who is accessing them** **•Cyber and physical worlds converging**
High profile losses
•Boards become aware of the risk and losses they face
Hacking is no longer a hobby
•Hackers no longer compete for bragging rights –it's employment **•A hacker can afford many months and channels to steal high value assets**
The rise of the collective
•Dogma based "hactivsim" is easily perpetrated **•Hackers coming together in the name of the collective**

(**Source**: BT, HSRC)

❑ The bulk of the cybersecurity market is orientated around large commercial enterprises securing their day-to-day business. This would include banks, telecommunications companies; utility and energy firms, manufacturers and retailers, and its constituency comprises the largest firms indigenous to or operating in the Banking, Financial Services, Retail & Payment Services industry cybersecurity market. Some of these firms have a role to play in the nation's critical national infrastructure, but the nature of the threat is considerably less than that for intelligence and defense organizations.

❑ The U.S. administration supports information gathering actions by businesses such as the insurance industry to evaluate cybercrime threats costs and inspire the progress of cybersecurity insurance services. The realization of such an endeavor is critical to implement cyber insurance programs and reduce the financial effect of cyber-attacks.

- Most small and medium-sized banking & financial services businesses (over 16.000 organizations) have cybersecurity needs, but these are substantially less in sophistication and scale to those experienced by larger financial organizations. Similarly, financial services customers and many suppliers have cybersecurity necessities but are at the low tier of the cybersecurity spectrum.
- Recent business models are rapidly evolving as financial sector employees conduct more of their work offsite. Protecting data and people who have access to it has become a challenge, costing clients time and money as super-secured identity and access management products enter the market. This product line combines proven software and analytics technology with expert managed services that make it easy and safe for financial sector businesses to tackle the complexities of security.
- Under the burden of more government regulations and increasing sophistication of cybersecurity threats, banking & financial services are demanding that IT and cybersecurity vendors implement access governance policies and solutions that provide visibility into operational and IT risks.

"Cyber Attacks are the "New Normal" for Financial Services Industry."

Wall Street Journal

- From a supplier point of view, it is vitally important to understand the characteristics of the banking & financial services industry cybersecurity market.
- Clearly, selling into the defense and intelligence market is entirely different to doing business with the banking & financial services industry. But this research shows that it is just as different selling into banking & financial services industry as it is into the public sector (even beyond the defense and intelligence elements). The sophistication and scale of the cybersecurity requirements, the credentials and clearance requirements, and the way in which each submarket procures cybersecurity capability are all substantially different in each submarket. Suppliers to the banking & financial services industry cybersecurity market, therefore, need to understand the dynamics of the banking & financial services industry cybersecurity market, and to adjust their go-to-market approaches accordingly.
- It is also important for cybersecurity suppliers to understand the potential in their market of choice. The size of each submarket varies considerably and the predicted growth rates are also quite distinct.
- The smallest submarket, but the most mature, is the defense and intelligence segment. It has been using cybersecurity technologies for many decades and is by far the most sophisticated user of such

technologies. However, despite a common perception to the contrary, this submarket is not large, the market costs of entry (such as Commercial Product Assurance certification) are high, and the rewards are uncertain.

- Behavior Anomaly Detection provides the ability to detect threats that are not part of a known pattern or signature, but which are unusual or unexpected. It's vital to defend against newer or targeted attacks.
- The two largest sections of the markets are the banking & financial services market enterprise submarket and the 'other' monetary public sector segments. These submarkets have similar cybersecurity requirements and they both feature considerable scalability requirements across their organization structures. For example, the security requirements of the DWP's benefit payments system are not dissimilar to those of a bank. There are also similarities in the role these types of organizations play in providing critical national infrastructure.
- There are differences in the maturity of elements within these submarkets: banking is particularly advanced due to its long history of security and more recent regulatory requirements. But, importantly, the skill set requirements for cybersecurity expertise migrate easily between these two submarkets.
- The submarket with the lowest level of maturity in cybersecurity banking & financial services industry is the industry's small/medium-sized organization and financial consumer segment. This is significantly underserved by the cybersecurity industry, although this is largely driven by the low levels of demand from buyers. In fact, a major issue for the industry is the markedly low level of awareness, education and understanding of the threat to business and personal information from insufficient cybersecurity measures.
- A particular issue for suppliers to the small/medium-sized organization and financial consumer segment is the free (to acquire) or bundled nature of the basic cybersecurity products from Microsoft, AVG and others. It means that revenues to be gained from anti-virus, firewall and other such foundation technologies are constrained.
- There are two reasons for this: driving up adoption of cybersecurity best practice increases a national stature as a safe place to do business, and increasing demand also drives the cybersecurity supply-side. We also found that the major beneficiaries of this increase in demand will be small/medium sized suppliers of cybersecurity advice and services.
- One of the key barriers to cybersecurity growth is the availability of skills. This shows up in a number of ways, from the low numbers of professionally accredited practitioners to the relatively high salaries commanded by those with experience. Limiting factors on skills include low levels of STEM graduates, a lack of attractiveness of careers in

cybersecurity, and a disconnect between university syllabuses and firms seeking raw talent.

- The threat of cyber-attacks and data breaches looms large for banking & financial services organizations of all sizes. Faced with this risk its imperative that banking & financial services firms adopt a holistic approach to combating cyber-security threats. This includes a deeper understanding of what makes them vulnerable to attacks and a comprehensive plan to protect themselves from future threats.
- In addition to hiking internal security measures, banking & financial services firms must also be concerned with the security of their vendors, service providers and other third parties.
- To properly defend themselves against cyber threats, banking & financial services organizations implement a proactive and comprehensive technology plan. This includes a data loss prevention solution, as well as encryption software, web proxies and a malware filtering solution to weed out legitimate emails from phishing and whaling emails, which represent about 80% of incoming emails.
- Any financial company that stores Personally Identifiable Information (PII) locally or on a cloud server faces the risk of a breach. Whether the PII was lost or stolen, the costs in dealing the breach can be substantial. Coverage for these types of losses is not covered under typical commercial insurance policies and need to be addressed separately.
- By 2022, 80% of banking & financial services industry including the retail & whole sale sectors information security funding will be allocated for rapid detection and response, up from 12% in 2014
- The U.S. leads the way in cybersecurity spending with its enormous budgets, albeit its expenditure as a proportion of overall IT spending is similar to the UK or Germany
- The U.S. has the tech companies with the deepest pockets; Amazon, Apple, Google, Microsoft, Intel and others, who lead the way in R&D spend on cybersecurity solutions linked to their general and financially related IT offerings applicable to a large degree to all markets: consumer & SMB, large enterprise, government and military.
- The US leads the world in large generalist cybersecurity service and platform providers such as IBM, HP and Accenture, who have strong cybersecurity teams.
- The US has a much better developed system of growing innovative tech startups (of all kinds) into medium and large companies through a much larger, more adventurous and more mature system of venture finance.

- France spends proportionately more on defense than the UK; it also has a cyber-security sector of similar size and shape as the UK, and a strong program of promoting homegrown solutions
- France stands out for its strong generalist IT service providers – Capgemini, Atos, Steria which have strength in this area sufficient for the needs of most mid-large sized enterprises which they can leverage with their clients around Europe
- France is having success in getting its multinationals to pull in small/medium-sized enterprises as partners in cybersecurity projects
- Israel stands out as a leader in small specialists; due to its geo-political position, it has a very focused agenda to produce leading-edge solutions for the military/intelligence community (although there is a long history of its best startups being acquired by larger overseas players mainly in the US).
- Japan is the second-largest spender on IT security solutions, both in absolute terms and as a proportion of overall IT spending.
- A number of global-scale, defense-oriented contractors, with world-class skills and recognized track records in general security and cybersecurity
- A strong traditional defense industry whose business can be leveraged to sell cybersecurity to those countries and organizations where that traditional business is strong.
- Hundreds of small services and products providers with good and sometimes unique knowledge and IP in cybersecurity.
- The fifth largest and arguably the second most mature market for IT products and services in the world, with particular pockets of need like banking & financial services in the City of London; thus there is a proportionately high demand from organizations for cyber solutions to meet their particular needs
- A vibrant tech industry, particularly in certain specialist areas like mobile applications development centered in London, which will require local and often specialized support.
- Many banking & financial services in small/medium-sized enterprises have a view that (security breaches) will never happen to them. The problem is they are now the low hanging fruit for the hacker as the larger organizations are becoming more difficult to compromise. Most small/medium-sized enterprises are also unaware of what defenses they can use to make sure they are more secure.
- Strong research, knowledge and track record in its universities supported by government – but, very importantly, a poor track record in commercializing that research, and widespread indifference amongst

small/medium-sized enterprises towards using the results of academic research in their own businesses.

- A growing awareness in the business and IT community at large about the importance of cybersecurity (albeit less knowledge on how best to respond).
- The challenge for the cybersecurity sector and for each government is to protect and nurture the industry, as there is considerable potential at home and overseas to be exploited business and that if one country doesn't acquire it, overseas companies surely will.
- Importantly, there has been an expectation in the past of a "trickle-down" effect in cybersecurity – that sophisticated solutions developed for defense and critical infrastructure providers will in due course be required by those further down the 'hierarchy of needs' and their developers will benefit from a wider market. However we find little evidence of that. It seems rather that large scale IT providers (mainly in the US) will incorporate the ideas and bundle them in their own products and services to service the less sophisticated needs of general enterprise, and then of consumers and small/medium-sized enterprises.
- Growing Internet penetration and rising popularity of online banking have made Japan, the US and India favorite countries among cybercriminals, who target online financial transactions using malware.
- For example in May 2014 alone, it saw 13,000 malware infections. In the same month the US saw about 5,000 malware infections, followed by India at 3,000 attacks.
- Japan tops the list with the highest number of online banking malware infections due to Vawtrak.
- The malware payload is Vawtrak also known as Neverquest, a backdoor and a dangerous banking Trojan able to spread itself via social media, email and file transfer protocols. Vawtrak can recognize hundreds of financial institutions and contains a function that monitors certain keywords, allowing the cyber criminals to expand the list of targeted banks.
- Vawtrak can modify the content of a web page and inject rogue forms on bank sites. Once the threat lifts the credentials of a bank, they send it back to the C&C. The hacker can use a VNC (virtual network computing) server to take control of the compromised computer and can login into the bank account via the compromised computer to perform the theft.

More information can be found at:
U.S. Financial Services: Cybersecurity Systems & Services Market – 2016-2020