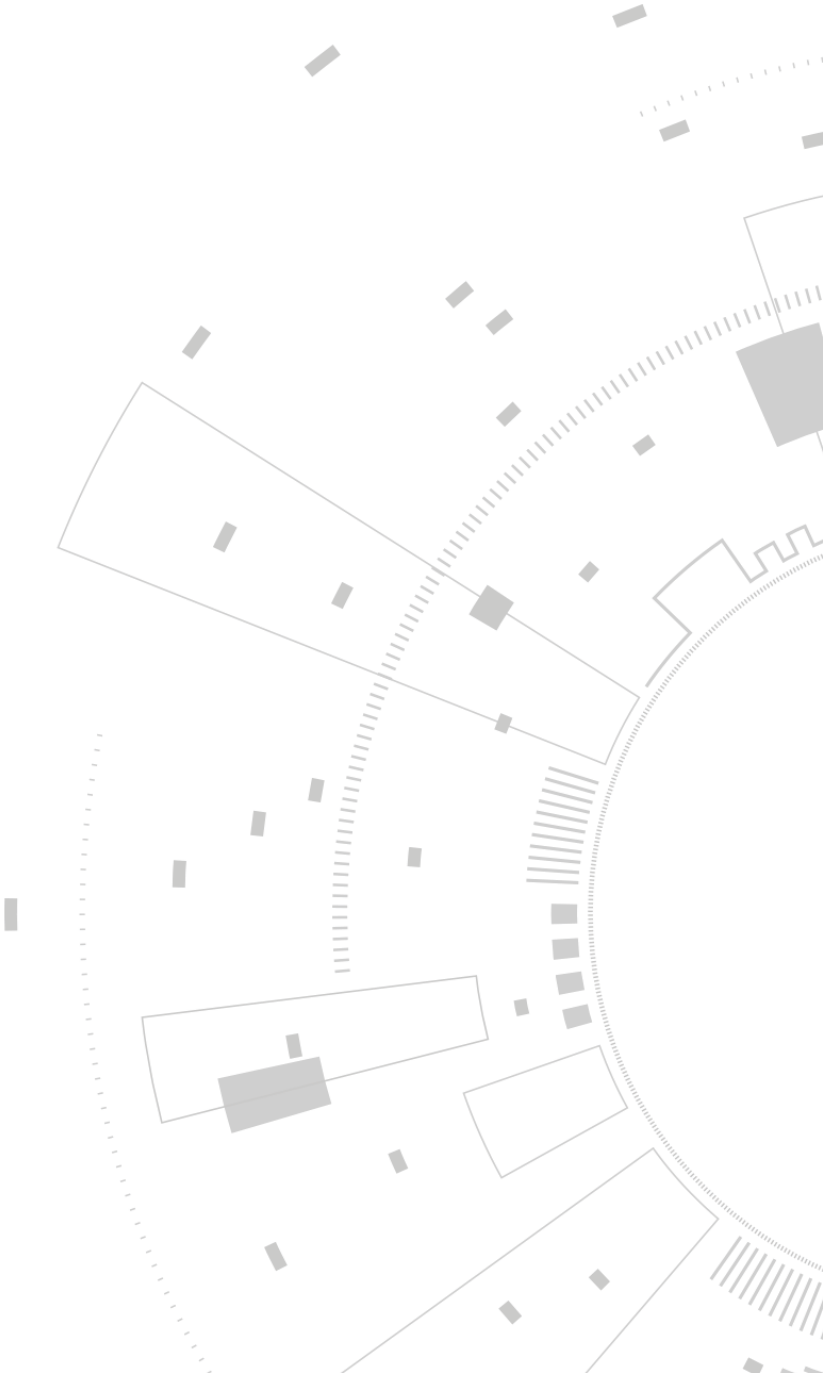

THE
FLOOR
CYBERSECURITY
& FINANCIAL
INSTITUTIONS
VIEWS FROM INDUSTRY PLAYERS & THE CYBER NATION

CONTENTS



EXECUTIVE SUMMARY

The financial services industry is going through a revolution. New technologies are refreshing old banking traditions and providing a multitude of opportunities for financial institutions to serve new markets, reinvent the way they interact with customers and conduct their operations.

These opportunities are, however, accompanied by unprecedented risks. As individuals move their lives online and global commerce digitizes, the volume and complexity of digital transactions have increased. A growing cyber interdependence has resulted in heightened global risk and left financial institutions to deal with a broad array of interconnected cybersecurity threats.

A new reality has dawned. Today's financial institutions operate in a high threat level environment where they must defend against a growing number of persistent, well funded, and highly sophisticated adversaries. It is no longer a question of if, but rather when a cyber breach or hack will occur.

The bad news is that cybersecurity will become more challenging as the Internet of Things increases the number of digital transactions to previously unimaginable levels. New regulations like PSD2, while enabling banks to leverage complementary strengths of fintech startups, will also add to security concerns as third parties join into the ecosystem of assets that must get protected. At the same time, financial institutions must alleviate a skills shortage and education gap that is impeding their ability to defend against cyber criminals.

Ultimately, the complex and multifaceted nature of cybersecurity challenges will compel financial institutions to re-envision their entire cybersecurity outlook. This will require industry collaboration, the utilization of new technologies and the implementation of dynamic strategies which enable the creation of capabilities that exceed today's business needs and meet tomorrow's innovation.

MAJOR CYBER SECURITY CHALLENGES

Today's cybercriminals are well funded, persistent, innovative and have more opportunities than ever before as the digitization of financial services offers up an increasing amount of high-value targets. In this high threat level context, financial institutions have no option but to continue to evolve their approach to cybersecurity. This will require going beyond technological issues which have traditionally received the lion's share of attention.

EDUCATION, HUMAN CAPITAL & INDUSTRY COLLABORATION

Thinking about cybersecurity through a single IT paradigm is no longer sufficient. Cybersecurity is as much a people issue as it is a technology issue. Cybersecurity strategies, therefore, require the implementation of the right technologies as well as a highly trained and educated workforce to be effective.

Despite considerable security concerns, weak BYOD and BYOA policies have been adopted across the financial industry. While many institutions are implementing forward-thinking policies, the severe threat level and diverse nature of attack vectors mean that nothing short of an organizational-wide culture of continuous learning will suffice. Malicious and inadvertent insider incidents made up just under 58% of all attacks on financial services firms in 2016, with unintentional actors making up 53%.[1]

It's not only employees acting with malicious intent that are causing cyber incidents. Careless employees that lose or share their passwords, open infected emails or misuse data are also inadvertently causing problems for financial institutions.

Employees at all levels must understand current threats, be trained to spot suspicious activity and get provided with the right (secure) tools to do their job. But education is a two-way street. Beyond focusing on employee education, there is a need to educate customers on cyber best practices as well.

"The human angle is a weak link, due to employees and customers opening infected links in emails, losing unlocked phones, transferring files from DOKs to their devices, and so on. However, digitization is not only about banking. It is also, for example, about IoT. Home appliances provide an additional attack vector as they are connected to banks."

Yair S. Finzi-
Co-Founder & CEO, SecuredTouch

Before this transformation can occur, leaders at the highest levels of financial institutions, including the board of directors, must comprehend the dynamic nature of cybersecurity, and the movement of cybersecurity from a mainly IT-based risk to a business and operational risk.

Organizations that have a mature security program will require the CISO to report to CEO, CFO, and other senior executives continuously. All C-suite level executives, not just CISOs, must play a leading role in cyber governance, risk assessment, monitoring structures, and intelligence sharing with relevant teams across organizational, sectoral, and national borders.

Effective leadership will also demand sustained action to address a severe shortage of qualified cybersecurity professionals. A skills gap analysis from ISACA estimated a global shortage of 2 million cybersecurity professionals by 2019.[2] This deficit is expected to worsen in size and impact as organizations scramble for talent to fight against a growing tide of cyber threats. By 2021, it is predicted that there will be 3.5 million unfilled cybersecurity job openings.[3]

The utilization of data analytics and automation based technologies to scale security efforts will be part of the solution. Financial institutions will, however, be required to find ways to nurture and attract new talent, provide career pathways and continuous retraining. If institutions are unable to close the skills gap, they will be forced to outsource more of their security to third parties which will introduce an entirely new set of challenges and risks.

The severity and scale of cyber threats together with industry-wide interdependencies also necessitate inter-organizational collaboration for the greater good. Financial institutions that share intelligence and experiences to fight cybersecurity threats will be more secure. Voluntary efforts such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) establishing the Financial Systemic Analysis & Resilience Center (FSARC) and the Global Resilience Federation should be encouraged and expanded.

REGULATIONS

Realizing the gravity of the cyber threat, regulators around the world are stepping up their diligence on financial institutions and third parties and are mandating tougher cybersecurity standards. The New York Division of Financial Services (NYDFS), for example, promulgated substantive cyber regulations that require financial institutions to have appropriate assessment and evaluation programs in place as well as protections for customers, employees, IT and business information. Financial institutions are now also obliged by law to have more stringent systems to guard against the disruption of business operations as well.

The adoption of the revised Payment Services Directive (PSD2) has set the stage for a new era of open banking in Europe. In 2018, PSD2 is set for implementation across the European Union requiring banks to open their infrastructure to third parties while still bearing the responsibility for cybersecurity.

The emergence of PSD2 will dramatically test the financial industry as new exposures from third-party vendors, many of whom are weak in the area of cybersecurity come to bare. A more open infrastructure could potentially lead to an increase in cyber attacks and hefty penalties unless financial institutions can protect all their digital assets and implement comprehensive security protocols and standards.

The EU General Data Protection Regulation (GDPR), also due to be implemented in 2018, will change the way that organizations handle, store and protect data. GDPR presents the most significant change in global privacy laws in decades and will require financial institutions to tighten up their cybersecurity processes and procedures or face financial penalties.

GDPR places new obligations on any business that handles the data of individuals living in the EU, independent of where the business is located. Financial Institutions that operate in the EU will need to ensure that all appropriate measures are taken to protect their customers' data. Robust incident response plans will have to be implemented to enable institutions to act quickly and mitigate any loss of data.

Adding to these regulation sets, the European Union's Directive on Security of Network and Information Systems (NIS Directive) introduces new security measures and incident reporting obligations for operators of essential services (OESs) in critical national infrastructure (CNI) and digital service providers (DSPs).

The NIS Directive has been adopted by the European Parliament. EU member states have until the 9th of May 2018 to transpose it into national laws, and an extra six months to identify the operators of essential services to which it applies. Banking and financial market infrastructures will be affected. The UK government has confirmed that the NIS Directive will apply irrespective of Brexit.

STRATEGY & TECHNOLOGY SHORTFALLS

A greater number of digital services, more substantial reliance on third-party partnerships and a highly interdependent financial industry are increasing the scope and complexity of security challenges. Today, an attack on one institution or third party provider does not necessarily mean impacts are confined to that one organization. Cyber attacks directed at one institution can impact multiple financial institutions and entities throughout society in a multitude of ways.[4]

While there is growing acknowledgment among cyber professionals that cyber attacks today are all but inevitable, gaps in cyber resilience strategies are becoming more evident. As sense related protections - the ability to predict and detect cyber attacks, and resistance protections - the ability to fend off attackers have improved, reaction and attribution capabilities continue to lag[5]. Many financial institutions also continue to be overly focused on external threats, despite research indicating that insiders are often more likely to be the source of a cyber attack.

In an environment where cyber attacks are all but inevitable, more attention and investment is needed to prevent attackers escaping with critical information and assets, finding those responsible and developing robust incident response mechanisms to ensure business continuity. Impending regulations like PSD2 also mean that conducting ongoing risk assessments and stress-testing interdependencies is a vital part of all financial institutions cyber preparedness.

WHAT ARE THE GREATEST MANAGEMENT AND/OR HUMAN RELATED CHALLENGES IN THE CYBERSECURITY DOMAIN?

"The greatest challenges I see today in the cybersecurity domain are:

- The integration of the cyber security and privacy risks and regulatory requirements in the overall organization strategy, organizational structure and plans.
- Creating cyber security awareness throughout an organization and leveraging every employee and stakeholder as part of the cyber security framework.
- Recruiting, training and retaining high-level cyber security practitioners.
- Acquiring up-to-date cyber threat intelligence and leveraging it immediately to protect organizational assets.
- Deploying the correct cyber security controls (People, Processes, Technology) and maintaining the deployment over time."

Doron Tamir, Brigadier General (Ret),
Israel Defense Forces

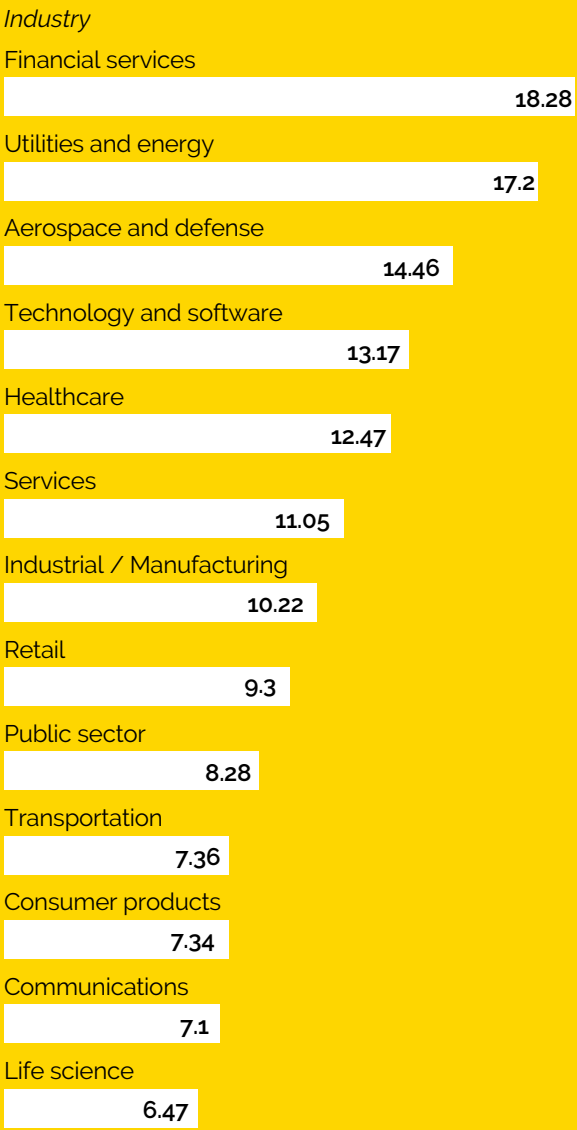
THE CYBER ATTACK LANDSCAPE - CURRENT & EMERGING TRENDS

The proliferation of digital omnichannel services together with more substantial reliance on third-party partnerships is making the threat landscape more challenging.

Calculating the total cost of cybercrime remains a difficult task. While it is possible to measure the tangible damage caused to data and systems, or financial payouts, it remains much more challenging to quantify intangible elements like the cost to an institution's brand, customer relationships and loss of IP. Despite the financial industry making great strides forward, cybercrime costs financial service providers more than any other sector. The rate of breaches is rising quickly, tripling over the past five years, according to a report from Accenture and the Ponemon Institute.[6]

It is estimated that the global cost of cybercrime will reach US$6 trillion annually by 2021, with the financial industry incurring a significant share.[8] What's more important, beyond these estimates, which vary considerably, is that executives in the financial industry fully internalize the gravity of the cyber threat.

Average annualized cost of cybercrime by industry sector (US$ million). [7]



Source: Accenture 2017 Cost of Cyber Crime Study

HOW WOULD YOU DESCRIBE THE CURRENT CYBERSECURITY THREAT LEVEL FOR FINANCIAL INSTITUTIONS?

"FIs are known to be exposed to the highest risks as a cyber crime target when compared to other industries due to the amount of personal data managed as well as direct financial benefits expected from attackers. Threats from cyber crime continues to grow. PwC 2016 Global Economic Crime and Fraud Survey indicates that 49% of global FIs have encountered a cyber attack, out of which, 37% of FIs resulted in financial loss. With FIs more actively pushing their service offering to digital first, mobile first, and even open banking, it opens up more entry points or vulnerabilities to be explored by attackers. We expect that this trend is unlikely to go down in the future."
CTBC Financial Holding Cyber Team

"The current cybersecurity threat level for banks is relatively high. Banks lack full control over their customers' activities as a result of BYOD and private equipment policies that permit logging into a bank's website and into accounts. Authentication, privacy, and lack of security on end-user devices is becoming increasingly challenging. Banks need to maintain their critical infrastructure, and continue to serve their customers, even when under attack."

Jacob Mendel,
General Manager Cyber Security COE, Intel

THE CYBER ATTACK LANDSCAPE - CURRENT & EMERGING TRENDS

Today's cyber landscape has a growing number of attack vectors. These can stem from a broad array of internal and external sources, last for a wide variety of time, and impact assets from ATMs and online banking services to core backend banking systems.

WHICH CURRENT CYBERSECURITY THREATS POSE THE BIGGEST RISKS TO FINANCIAL INSTITUTIONS?

"Definitely ransomware, and not only in its current existing format. Ransomware prevents the sending and receiving of information. It is essentially a "hostage situation." Ransomware "hostages" are finding it difficult to pay as payments can be tracked, but not so with cryptocurrency as it makes transferring funds easier, due to the anonymity inherent in digital currency. The parties involved will attempt to find the right praxis, based on factors such as cost of attacks vs. cost of defense, and risk appetite vs. risk tolerance."

Daniel Bren, Former First Military Joint Chief Cyber Defense Officer, Israel Defense Forces

MALWARE

Ransomeware, Adware, Bots, Bugs, Rootkit, Spyware, Trojan Horse, Virus, Worms, Brute Force Attack

SOCIAL ENGINEERING

Phishing, Spear Phishing, Pretexting, Baiting, Quid Pro Quo, Tailgating

MAN-IN-THE-MIDDLE

ARP Poisoning, WiFi WEP/ WPA/2 Hacking, DNS Spoofing, STP Mangling, Port Stealing

DENIAL OF SERVICE (DoS)

DDoS, Application Layer Attacks

EMERGING THREAT TRENDS

TARGETED FINANCIAL HEISTS & ADVANCED PERSISTENT THREATS (APTS)

Historically, cybercriminals have primarily engaged in indiscriminate hacks with a goal of taking a little bit of money or data from a large number of people or organizations. While these types of attacks continue, today, an increasing number of cybercriminals are focusing their efforts on where they can make the most significant impact. Well-funded and skilled crime organizations and state actors are conducting sophisticated and large-scale targeted financial heists at financial institutions around the world.

While many criminals are attempting to gain access to targets that deliver massive rewards from a single heist, some are also looking to conduct targeted attacks for non-financial gains, to disrupt and destroy the systems financial institutions rely on to operate. Whether for a financial or non-financial benefit, cybercriminals are willing to expend vast amounts of time and money to penetrate systems and cause damage.

Advanced Persistent Threats or (APTs) - recurrent low profile attacks that slowly penetrate a network, require patience, planning, and funding and can take an extended period to discover. Organized criminal groups or state actors typically commit APTs and as their name suggests, are advanced and persistent.

Despite targeted APT attacks having a lower success rate, the increased frequency of this type of attack represents a dangerous shift due to the potentially severe impact they can have on a financial institution.[9]

BANGLADESH CENTRAL BANK

In early 2016, criminals orchestrated a massive heist on the Bangladesh Central Bank. The offenders attempted and almost succeeded in transferring US$1 billion to selected accounts in Sri Lanka and the Philippines.

The hackers exploited weaknesses in the bank's security to infiltrate its system and gain access to computers connected to the SWIFT network. The attackers then gained control of trusted employee's credentials to make fraudulent money transfer requests through the SWIFT network, ultimately managing to get $81 million via four different transfer requests. The hackers began the heist at the start of a long weekend in Bangladesh to reduce their chances of getting caught. They also utilized malware to alter the bank's confirmation messages to delay the discovery of the transactions by bank employees.

FIRST COMMERCIAL BANK ATM HEIST

A network of well-coordinated criminals from Eastern Europe and Russia infected dozens of ATMs operated by Taiwan's First Bank. The malware files instructed the ATMs to "spit out cash" and delete evidence of the crime. Masked thieves walked away with bags of cash totaling around US$2.5 million in a matter of minutes, forcing banks to freeze withdrawals from hundreds of ATMs.

International cybersecurity investigations firm Group-IB has connected the hack to an international syndicate code-named “Cobalt” linked to attacks on ATM networks throughout Europe and Asia.

INSIDER THREATS

Cyber attacks conducted by individuals who maliciously betray their positions of trust and use their access for illegitimate means as well as incidents where individuals accidentally mishandle critical information or cause damage to a financial institution are on the rise. According to the IBM X-Force Threat Intelligence Index 2017, more than half of the breaches suffered by financial services companies were perpetrated by insiders.

Insider attacks can span from IT sabotage and fraud to theft and unauthorized disclosure, and can be conducted in hundreds of different ways.

Despite insider threats causing some of the highest impacts and accounting for a significant percentage of cybersecurity incidents, many financial institutions remain ill-equipped and vulnerable, as they continue to focus their resources on traditional network defenses that fail to prevent attacks initiated by insiders.[10]

CURRENT & EMERGING TECHNOLOGIES

The scope and scale of security threats today far exceeds the capacity of even the most skilled security teams. The good news is that current and emerging technologies show great promise to assist financial institutions in their fight against cybercrime. These technologies will need to be leveraged by financial institutions to scale cybersecurity efforts, defend against new and sophisticated threats, and ultimately enable the continued provision of digital innovations.

WHICH EMERGING TECHNOLOGIES DO YOU THINK WILL BRING NEW THREATS TO FINANCIAL INSTITUTIONS?

"I don't see new emerging technologies being a specific risk from a cyber perspective (although the increase in the internet of things etc. will bring new attack vectors), but changes in the ways of working (SaaS / PaaS etc.) brings new challenges along with an increase in mobile computing, etc."

Chris Ulliott, Chief Information Security Officer, RBS

BIOMETRIC AND BEHAVIORAL AUTHENTICATION

The friction between customer security and customer experience is increasing. Today's consumers are demanding streamlined, user-friendly applications, accessible on any device, at any time and from any location. This is causing difficulties for financial institutions as they battle to implement effective security processes that do not impede customer experiences.

Behavioral authentication technologies can deliver financial institutions the ability to identify each customer's unique behavior and interaction patterns by collecting information about a customer over time and creating a user profile. Everything from search and use habits to how a customer types and scrolls when using their device can be analyzed.

After developing a user profile, financial institutions can better protect their online and mobile retail banking services, gaining the ability to automatically identify unusual customer behavior and alert both customer and institution in real-time. By helping to distinguish the actions of a cybercriminal from those of a trusted user with increased accuracy and efficiency, there is an opportunity to reduce fraud and prevent other types of cyber crimes from occurring while also reducing friction during a customer's online experience.

Biometric authentication technology has significant benefits for financial institutions as well. User authentication software that recognizes unique biological characteristics like facial contours and fingerprints can be used to authenticate users before they log into accounts or internal critical infrastructure systems.

Biological features are very difficult to fake making the use of biometric technologies integral for more secure access. The technology removes the need to use sensitive data when logging into online banking sites and internal banking systems which will bring a new level of security and dramatically enhance KYC. However, biometrics is not a silver bullet. Additional processes surrounding the onboarding process must be secure and robust.

CURRENT & EMERGING TECHNOLOGIES

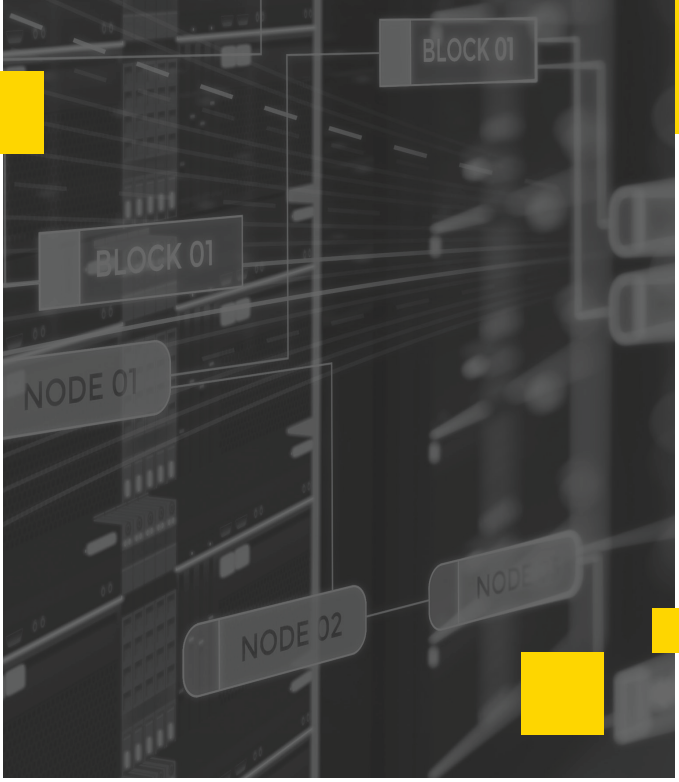
ARTIFICIAL INTELLIGENCE

The digitization of financial services has given financial institutions access to more customer data than ever before. However, these vast amounts of information have become more susceptible to cyber attacks and remain unstructured and difficult to analyze, making the utilization of data and the identification of suspicious behavior challenging.

Artificial Intelligence encompasses different technologies, such as machine learning, pattern recognition, and prediction. Using machines and systems that are programmed to think and react like humans, designed to manage specific tasks and evolve to handle any task is now integral to future efforts to fight sophisticated cybercriminals.

By leveraging Artificial Intelligence technologies, financial institutions can automatically analyze massive amounts of data resulting in a more advanced understanding of behavior patterns and anomalies. As more data is analyzed, AI-based systems become smarter and better equipped to detect suspicious activity and even anticipate future attacks.

AI promises to improve threat detection and amplify the ability of financial institutions, through automation, to investigate incidents and fight attackers at a time when massive data flows, digitization and a skills shortage is impacting organizations.



BLOCKCHAIN

Blockchain has created a tremendous amount of hype in the financial services industry in recent years. A blockchain is an immutable and tamperproof distributed ledger or decentralized database that keeps continuously updated digital records. The technology promises to provide financial institutions with game-changing cybersecurity abilities.

Blockchain delivers the ability to not only detect and defend against fraud and the manipulation of data, but it also dramatically increases the attribution capabilities of financial institutions. With a fraud prevention system based on an unchangeable record of auditable past transactions, financial institutions can prevent data manipulation, theft, and fraud from both internal and external sources.

Such technology can also provide significant enhancements to the verification and authentication of customer identities (KYC). By leveraging a distributed key infrastructure for authenticating devices and users, the potential to eliminate the need for passwords could finally be realized. What's more, through the removal of human factors from within the authentication process, several human-related attack vectors can be eliminated.

ISRAEL & CYBERSECURITY- A SUCCESS STORY

Over the last two decades Israel has become one of the most respected cyber technology powers in the world. The country has the second highest number of cybersecurity companies after the United States, an astonishing feat for a nation with a population of only 8.5 million.

In 2016, Israel's cybersecurity sector made up of approximately 365 companies, raised a total of $581 million, a 9 percent increase from 2015. The Israeli cyber industry represents 15 percent of the total venture capital raised by cybersecurity companies worldwide.

According to data from YL Ventures, 60 new cybersecurity startups launched in 2017, raised $847 million. Israeli cybersecurity companies, not including IPOs, exited for approximately $1.3 billion in 2017, with an average exit valuation of $130 million.

2017 ISRAELI CYBER FIGURES:

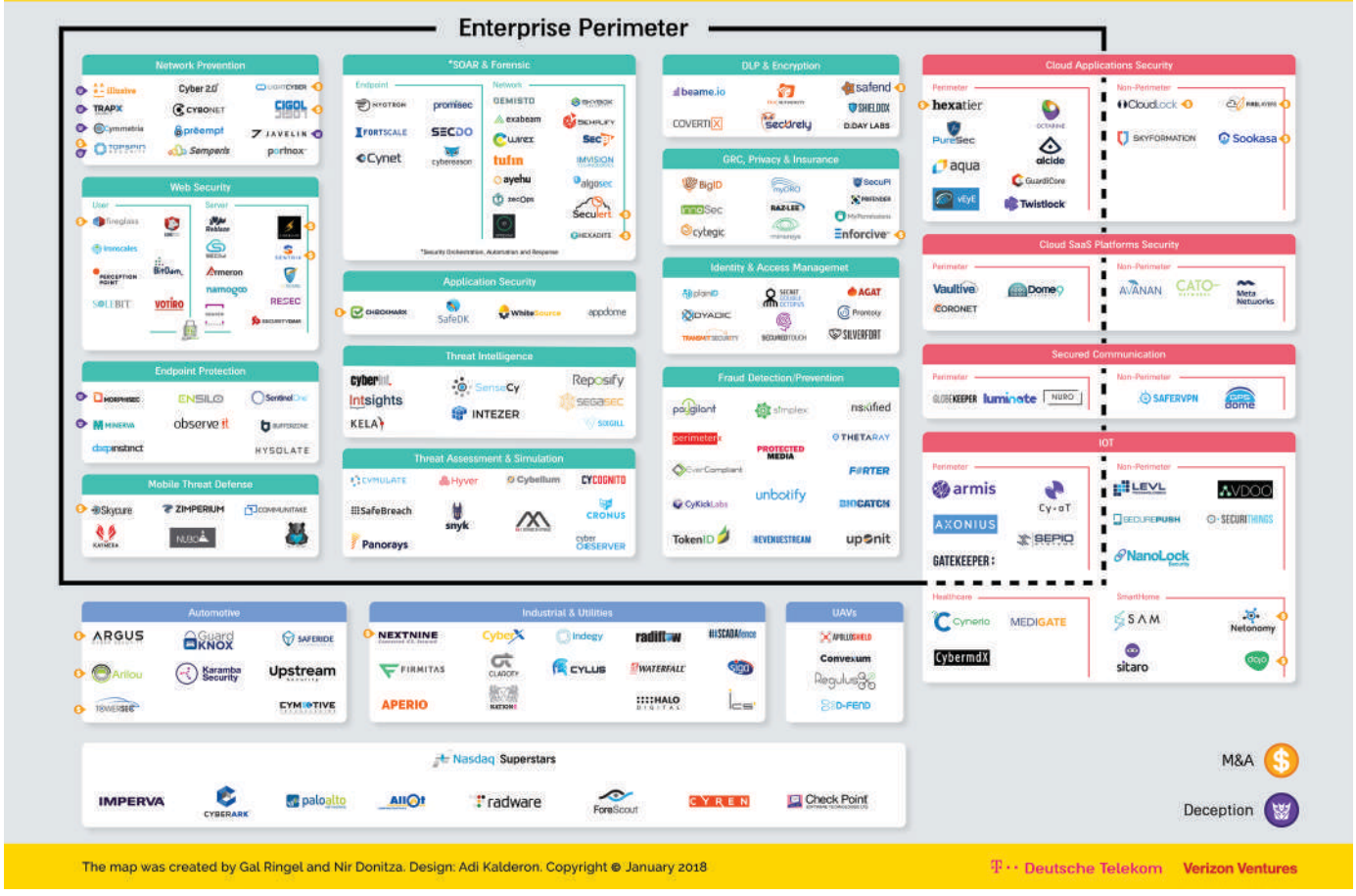
Israeli Cyber Security companies raised **$814.5M**

3rd year of record investments in a row - **18%** of the global investment, second only to the US.

14 companies had **$1.4B** in exits in 2017, also a new record.

30 international Cyber Security R&D centers in Israel

THE ISRAELI CYBERSECURITY LANDSCAPE



Source: Deutsche Telekom & Verizon Ventures

ISRAEL & CYBERSECURITY- A SUCCESS STORY

ISRAEL'S COMPETITIVE EDGE

Israel's success in the cybersecurity arena owes to a multitude of factors that stem primarily from the country's security and economic challenges. These challenges created a unique culture of entrepreneurship and innovation, and have led to the development of a world-class cyber-infrastructure which includes investment and coordination between organizations across society. In the past two decades, the Israeli government, academia, military, private sector and non-profit sector have taken unprecedented action to fight a rising tide of cyber threats.

CYBER INITIATIVES

Since the year 2000, as global cyber threats have multiplied and continued to impact Israel's strategic assets, the Israeli government, academia, private sector, and non-profit sector have nurtured the development of a cybersecurity industry that today has over 400 startups. These efforts have ensured that new generations of human capital are readily available to mold into the next cybersecurity professionals, experts, and startup founders.

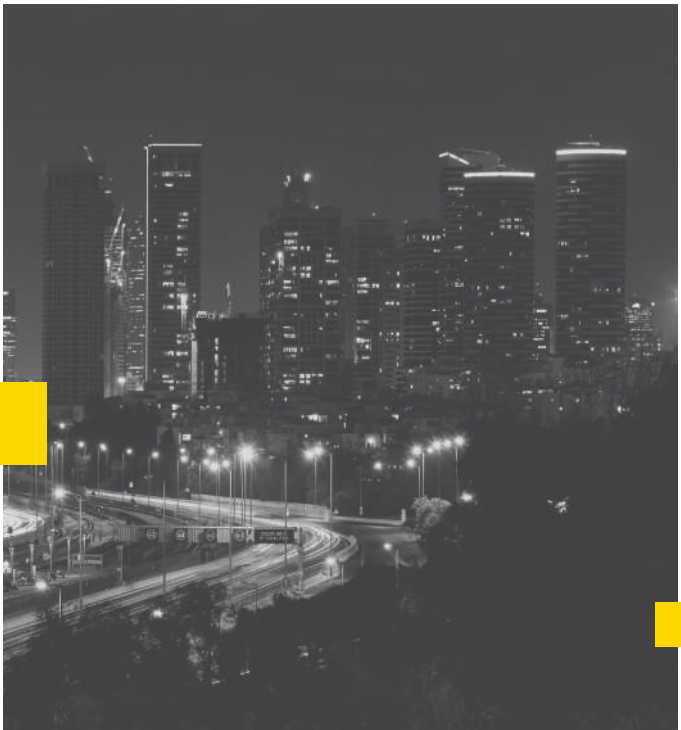
WHY DO YOU THINK ISRAELI COMPANIES LEAD THE WORLD IN CYBERSECURITY INNOVATION?

"By the end of 2017, there were approximately 420 active cybersecurity companies in Israel. The country is the world's second-largest exporter of cybersecurity products and services, after the US. There is a unique ecosystem in Israel with a pool of local talents, veterans from various elite cyber units with extensive expertise in both offensive and defensive cyber. These skill sets are combined with the innovation necessity to develop new technologies to protect the country which is under continuous cyber-attack."

Boaz Gorodissky,
Co-Founder and CTO, XM Cyber

"Cybersecurity started as a necessity due to national security and was then promoted by government and industry. Mandatory army services, including in elite intelligence units plays a large role."

Ishai Wertheimer, Partner,
Head of Information Security Services, KPMG



ISRAEL & CYBERSECURITY- A SUCCESS STORY

More than ten academic excellence centers have opened to develop innovative solutions for critical national infrastructure security, prevent cybercrimes and cyberterrorism and promote cybersecurity education across the country.

The National Cyber Bureau was established with a mandate to boost cybersecurity coordination and policy development at the highest levels and across industries. Israel's high schools offer cybersecurity as an elective subject, university students can study a Ph.D. in cybersecurity, and non-profit organizations like the Cyber Education Center have been set up to cultivate cyber interest and talent at an early age.

There is widespread acknowledgment in government and the private sector that cyber technology is not only an essential growth engine for the Israeli economy but a critical element in Israel's national security. This understanding has resulted in the country's unshakable commitment to growing the pool of highly-skilled cyber experts and remaining a leader in the field.

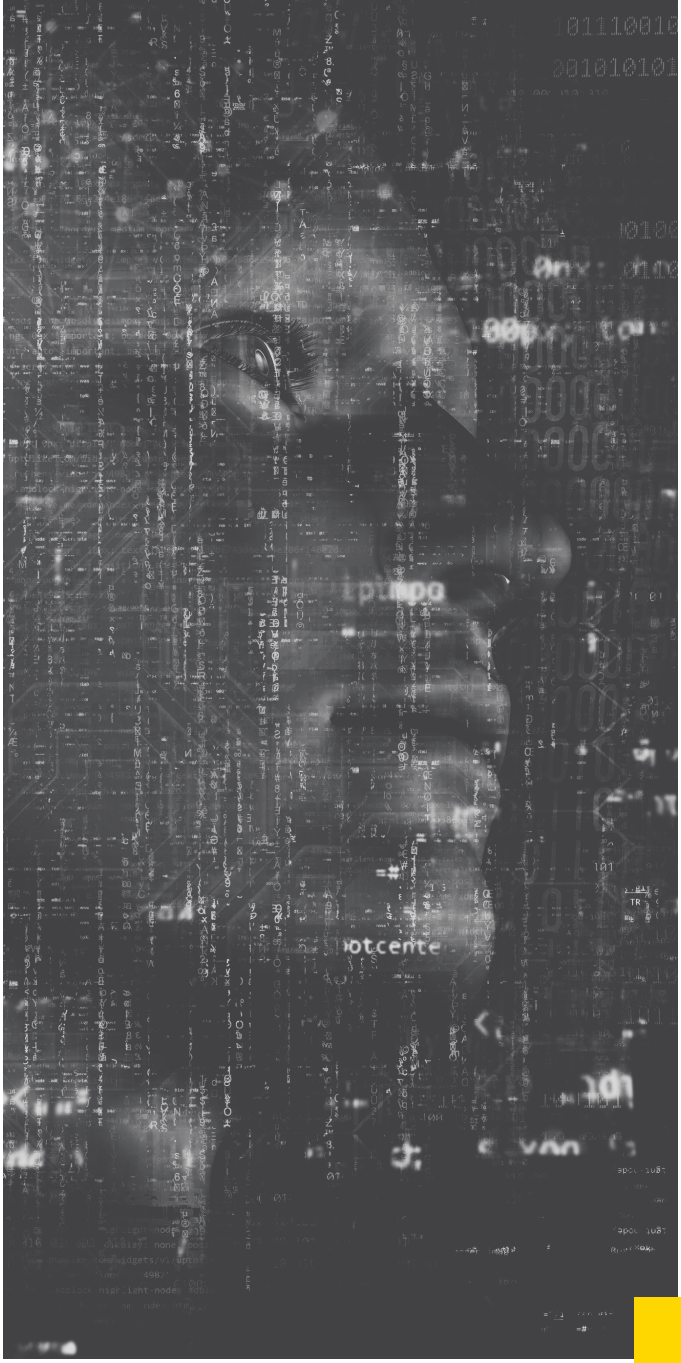
The government's policies and approach to cybersecurity are proactive, comprehensive and forward thinking. Combined with academia and the private sector, cross-societal initiatives make for a potent force in cyber education, investment and innovation.

ISRAEL & CYBERSECURITY- A SUCCESS STORY

MILITARY - CYBER NEXUS

One of the most critical elements that drive Israel's competitive edge in the cybersecurity realm is the military's ability to incubate talent and accelerate the transfer of knowledge to the commercial world. Soldiers are taught to innovate and build prototypes of advanced cyber technologies. Many of these technologies are developed further and privatized by soldiers after their army service.

Unit 8200 is an elite branch of the Israel Defense Forces which specializes in computer security and cyber attacks. The Unit has produced some of the country's leading cyber technology companies and is responsible for some of the world's foremost innovations in the cyber field.



CYBER SUCCESS STORIES

Israel's comprehensive cyber-infrastructure made up of government, academia, the private sector, non-profits and the military has driven the country to become a cyber powerhouse with world-class human talent and innovation pipelines.

It is this dynamic infrastructure that attracts global technology giants like CISCO, IBM, PayPal, EMC, Lockheed Martin and many others to choose Israel for their cybersecurity R&D headquarters and centers of excellence. A growing number of countries have also begun to recognize Israel's prowess in cyber innovation by signing knowledge sharing and collaboration agreements.

The country has produced a multitude of game-changing cyber companies, many of which have been acquired by leading companies or become global leaders. Today, Israeli cybersecurity innovations are critical to the enablement of organizations around the world to innovate and transition into the digital economy. In 2017 alone, a few notable investments include - Symantec's acquisition of Fireglass and Skycure, Microsoft's acquisition of Hexadite, Palo Alto Network's acquisition of Lightcyber and Germany's Continental AG's acquisition of Argus.

ISRAEL & CYBERSECURITY- A SUCCESS STORY

PAYPAL & FRAUD SCIENCES

In 2008, PayPal, purchased Fraud Sciences, a cutting-edge Israeli security company specializing in detecting online fraud, for US$169 million. Fraud Sciences developed technology that was able to differentiate between real and fraudulent transactions. The technology was implemented into PayPal's anti-fraud systems to increase the company's efficiency and harden defenses. The purchase of Fraud Sciences has had an enormous impact, helping PayPal reduce fraud rates and become one of the safest companies in the world.

IBM & TRUSTEER

In 2013, IBM purchased Trusteer, an Israeli enterprise security firm for approximately US$1 billion. Trusteer continues to help many of the world's largest banks and organizations defeat sophisticated attacks using advanced and innovative solutions that combine intelligence, cloud and mobile technologies.

CHECKPOINT

Checkpoint Software Technologies, an Israeli company specializing in network and data security has grown to become a global leader. The company serves many of the world's Fortune 100 and Fortune 500 firms as well as governments and other small-medium size organizations. The company is now the largest network cybersecurity vendor globally and is widely acknowledged to have an unmatched catch rate of malware and other types of threats.

A LOOK TO THE FUTURE

A LOOK TO THE FUTURE

While it's difficult to predict what the cybersecurity landscape will look like in the next few years, institutions should expect a challenging future. This future will see new technologies deliver financial institutions unprecedented abilities to revolutionize their services, but also dramatically increase cybersecurity risks.

Beyond the protection of critical business assets, cybersecurity plays a central role in enabling innovation. Without effective cyber protections, financial institutions will lose their ability to pass on innovative new services that have become a necessity for remaining competitive. In tomorrow's high threat level landscape, cybersecurity can no longer continue to be an afterthought when designing new financial services. Financial institutions must build cybersecurity into their new innovations from the beginning.

IN THE NEXT FEW YEARS FROM NOW, WHAT WILL BE THE KEY CYBERSECURITY CHALLENGES/ THREATS FACED BY FINANCIAL INSTITUTIONS?

"Cryptocurrencies and its vulnerabilities, alternative nonmainstream channels, different in-house protection systems, an un-holistic approach to cyber security, and diversified measures within financial institutions."

Shay Dovev, SVP Business Development and Sales, ThetaRay

"While governments and authorities continue to tackle cyber-crime, criminals will continue to seek out and exploit weak points. This is a fact of life in the connected world. In the financial service industry, with digital channels, fintech, and virtual banking models highly demanded by customers, threats will continue to rise and new cybersecurity models will emerge. FI's will need to focus more on customer centric security, customer identity access management, customer behaviour security and fraud analytics.

"At a minimum, organisations will need to measure their current strategies against other models and start remediating. Having a strategy and governance framework is one thing, but it's also important to have responsive capabilities. Most financial service organisations today have a crisis response team, however many of them do not simulate a real life cyber event. FIs need to engage with specialists to perform attack simulations and assess if people within the organisation know what needs to be done should a system get breached."

Henry Shek - Head of IT Advisory (Risk Consulting), KPMG China

"It's important that in the next years financial institutions improve their own cyber security competencies by investing in training and awareness for the staff, integrate cyber risk in the Enterprise Risk Management process and be prepared to better handle threats coming from the surrounding ecosystem where banks are going to operate"

Fabio Ugoste, Information Security officer, Intesa Sanpaolo

In the past, the implementation of new defensive technologies and the development of a limited and somewhat static multi-year best practice framework could deliver adequate protection of business assets. Tomorrow's cyber landscape, however, will be different. It will demand financial institutions to develop organization-wide cultures of security, agile and dynamic cybersecurity frameworks, and continuous customer and employee education. It will also require institutions to invest in cutting-edge technologies that can help enhance effectiveness and scale security efforts.

ABOUT THE FLOOR

The Floor, based at the Tel Aviv Stock Exchange (TASE), is a global Fintech innovation center working with six of the world's largest financial institutions.

The Floor operates a Reverse Innovation Platform through which it sources business pain points transformed into solutions from the Fintech ecosystem and its innovation labs. Empowered by its tier-1 bank partners, The Floor is shaping the "Bank of the Future" by leveraging exceptional technologies and expertise to provide its customers with the next generation financial technologies.

WITH THANKS TO:

- **Daniel Bren,**
  Former First Military Joint Chief Cyber Defense Officer, Israel Defense Forces
- **Anthony Back,**
  Fintech & Blockchain Analyst
- **Avi Cohen,**
  CEO & Co-Founder, The Floor
- **CTBC Financial Holding Cyber Team**
- **Shay Dovev,**
  SVP Business Development and Sales, ThetaRay
- **Yair S. Finzi,**
  Co-Founder & CEO, SecuredTouch
- **Boaz Gorodissky,**
  Co-Founder and CTO, XM Cyber
- **Intesa Sanpaolo Information Security & Business Continuity Department**
- **Jacob Mendel,**
  General Manager Cyber Security COE, Intel
- **Henry Shek,**
  Head of IT Advisory (Risk Consulting), KPMG China
- **Doron Tamir,**
  Brigadier General (Ret), Israel Defense Forces
- **Chris Ulliott,**
  Chief Information Security Officer, RBS
- **Ishai Wertheimer,**
  Partner, Head of Information Security Services, KPMG

[1] IBM-X-Force Threat Intelligence Index
[2] ISACA
[3] Cybersecurity Ventures
[4] PWC Global State of Information Security Survey
[5] EY Global Information Security Survey
[6] Accenture & Ponemon Institute Cost of Cyber Crime Study
[7] Accenture 2017 Cost of Cyber Crime Study
[8] Cybersecurity Ventures
[9] Symantec Financial Threats Review 2017
[10] IBM X-Force Threat Intelligence Index 2017