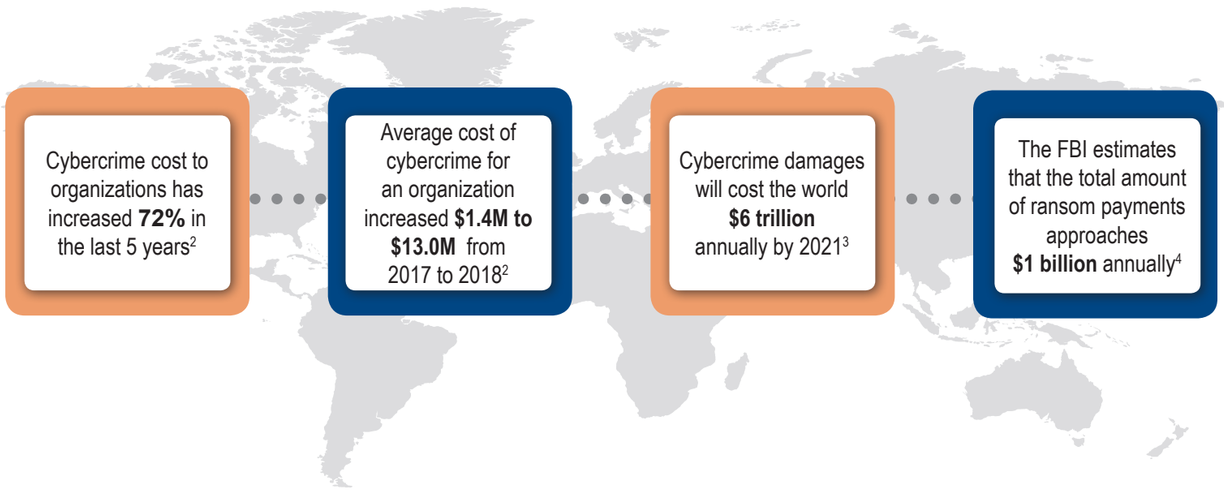
Cyber Resilience: Trends and Improving Preparedness

Impact of Cyber Security Breaches

Reputational impact, lost business opportunities, recovery costs as well as financial, staff time and productivity



[1] FBI, "Business E-mail Compromise: The 3.1 Billion Dollar Scam", 24 June 2016
[2] Accenture Security 2019 Annual Report "The Cost of Cybercrime"
[3] The 2019 Official Annual Cybercrime Report by Herjavec Group
[4] Department of Justice Deputy Attorney General Rod J. Rosenstein "Remarks at the Cambridge Cyber Summit" October 4, 2017

Diverse Risks and Trends Impact Resilience

Trend	Associated Risks
Increased Digitization	• Firms feel pressure to be "first to market" and "innovative"; many digital / growth strategies do not consider cyber • Increased tech usage and interdependencies create greater, less transparent, and more complex supply chain risks (e.g., 3rd / 4th Parties) • To reduce overhead costs, time-to-market, and improve incident response and resiliency, cyber needs to be more embedded in product lifecycle
Market Developments and Laws	• Siloed approaches to cyber, data privacy, data localisation, employment, and outsourcing laws impact incident response times and risk arbitrage • Public sector desire to attract investment and talent through initiatives only focused on innovation / new tech, this may create market risks or divergent standards • Market consolidation (e.g., M&A) generates cyber risks, such as insecure divestitures, incompatible tech stacks, staff exfiltrating data, unequal staff cyber education and culture
Growing Maturity of Cyber Risk Measurement	• Created by human adversaries; not the act of doing business nor frequency of a process • In a Data (trust) economy, financial assets and credit ratings increasingly serve as proxies for "value"; as they become less synonymous with the underlying reality, we need to explore how to better assess "Value at Risk", and asset / risk / deal prices, valuations, and credit ratings • Quantifying cyber risk and linking it's increase or reduction to the financial investment and spend on cyber controls remains challenging

The Cyber Threat Landscape

Nation-State Actors

Motivation: Theft of trade or craft secrets, or support of military capabilities, and nationalised industries

Methods: Using advanced malware to establish a foothold into infrastructure

Cyber Terrorists

Motivation: Instill fear to have targets comply with demands or ideology

Methods: Using SPAM, phishing, social engineering, malware, etc., to "enable" their programs (recruit, incite, train, and finance)

Hacktivists

Motivation: Seek publicity for their political agenda

Methods: Disruption (i.e., Distributed Denial of Service) and defacement

Insiders

Motivation: Emotional or sometimes financial needs

Methods: Uses insider knowledge to commit fraud, steal or manipulate data, conduct fraud, etc.

Cyber Criminals

Motivation: Make money

Methods: Spear-phishing and other techniques; mature underground economy supporting criminal activity

Methods

Ransomware | Web Downloads | Distributed Denial of Service
Social Engineering | Email Links & Attachments | Business Email Compromise (Phishing)

Sector-Neutral Common Threats: Business Email Compromise and Phishing

CEO or CFO impersonation by compromising an executive's email account or any publicly listed email is popular, however cyber criminals are shifting focus from C-suite to different employee groups, for example, HR, tax, and engineering.

The Cost of Email Scams

Average Remediation Costs for successful Spear Phishing Attack[2]	Global Losses Due to Business Email Compromise Scams[1]	Average Remediation Costs per successful Data Breach[3]
$1.6 Million	**$3.1 Billion**	**$4 Million**

[1] FBI, "Business E-mail Compromise: The 3.1 Billion Dollar Scam", 24 June 2016
[2] Cloudmark, "Survey Reveals Spear Phishing as a Top Security Concern to Enterprises", 13 June 2016
[3] IBM, "2016 Cost to Data Breach Study", 2016
[4] 2016 AFP Payments Fraud and Control Survey.

Payment Methods Impacted by Business Email Compromise[4]

Wire Transfers	56%
Checks	29%
Corporate/ Commercial credit cards	18%
ACH Debit	16%
ACH Credits	15%

(Percent of Organizations that Experienced Payments Fraud via BEC)

Cyber Resilience: Trends and Improving Preparedness

Preparedness Is Critical Across Your Organization

Executive Managers / Central Bank Governors

- Talk about areas of significant risk
- Understand assessment of threats and management's plans if a breach occurs
- Get regular updates on threats and defense strategy
- Conduct vulnerability evaluations

Finance Managers / Portfolio Managers

- Know cyber risks and their business impacts
- Communicate with seniors and global businesses to keep awareness of risks high
- Talk with key cyber partners on current threats
- Encourage team to leverage check list and toolkits

Risk / Communication Managers

- Be conversant on areas of significant risk
- Understand threats and have detailed knowledge of the communication plan
- Share updates on threats, approaches and business impacts with Executive Managers / Ministers / Central Bank Governors

Staff / Others

- Train regularly throughout the year
- Explore new technology such as gamification for training
- Practice cyber hygiene in the workplace and at home
- Subsidiary businesses need to build relationship in local markets with Ambassador from parent country

Best Practices Checklist: Protect, Detect, Respond

	People	Process	Technology
Protect	√ Staff Segregation of Duties √ Staff Training √ Identity and Access Management √ Accountability	√ Vendor Management √ Vulnerability Assessment √ Data Protection √ Cyber Fusion - a multi-disciplinary approach	√ Device/Software Controls √ Perimeter/Network Security √ Secure/Authorized Connectivity √ Rapid Patching and Response √ Apps and systems recovery time
Detect	√ Information Sharing √ Background Verifications √ Staff managing transactions must be able to identify a breach	√ End-to-End Processes √ Phishing/Vulnerability Disclosure √ Security Incident Management √ Audits and Reconciliations as Processes to Detect problems	√ Network and Endpoint Monitoring √ Leverage Automation and Robotics √ Regular gap analysis of capabilities
Respond and Recovery	√ External and internal comms back-up plan if phone / email no longer works √ Ensure all key participants have 1st, 2nd and 3rd delegate (crisis may last weeks)	√ Crisis Management plan including local media, press, and escalation to Executives √ Know thresholds for assets, liability, liquidity, and capital √ Local media / press communication plans √ Lessons Learned Review	√ Contingency plan for tech failure √ Regular System(s) Testing √ Assess Dwell Time, Mean-Time-To-Detect, Mean-Time-to-Respond

Select Citi Solutions: Services to Keep You Secure

CitiDirect®

Multilevel security and advanced data encryption technology features including, user entitlement and authorization, and tools to detect malware infection on client devices accessing CitiDirect®

CitiConnect®

Secure client system to bank connectivity for transactions and information with security controls that include message integrity, authenticity and nonrepudiation, monitoring of file delivery and processing, and data encryption

Citi Payment Outlier Detection

Proactively detect unusual payments in clients' transactions through data analytics, machine-learning algorithms, and receive near-real time alerts

Citi Payment Insights

Using big data, API, and the cloud, Citi Payment Insights has total access, visibility, and control with real-time payments visibility and the ability to action payments on-demand

Securities Services

Full spectrum of direct clearing and custody, global custody and funds services solutions with comprehensive control mechanisms that mitigate cyber risks. Our single, global platform is supported by robust network management with unified resolution and recovery plans, data protection, asset segregation and secure connectivity

Hedging / Risk Management

Bespoke resilience and risk management solutions across all asset classes including interest rates, foreign exchange, commodities, and equities

Agency Lending

Our follow-the-sun operations is supported by traders and services centers across the globe. We offer extensive in-market presence by diverse borrower pools in emerging and developed markets, with additional capabilities to tailor your program's parameters per your requirements (borrowers, securities, markets)

Liquidity Management Services

We minimize risk of internal and external fraud through multi-level approvals, vulnerability assessments, encrypted transactions, secure integration between internal and bank systems, and daily account reconciliation

Citi Cyber Security Advisory Toolkit

The Citi Cyber Security Advisory Toolkit provides a range of materials to help you develop a working knowledge of the threats, as well as the tools and techniques available to assist you defend your organization. Explore the Toolkit to learn more.

Visit: https://www.citibank.com/tts/sa/cybersecurity-toolkit/

What's New

- Cyber response planning checklist
- Thought leadership
- Cyber podcast

Overview & Articles

- Fraud Overview
- Cyber Response
- Slipsheet
- Managing Cyber Risk

Videos

- Citi Cyber Security Solutions
- Case Study: Beneficiary change
- Case Study: Impersonation

Guides and Best Practices

- Cybersecurity Awareness—Staff Training
- Beneficiary Change
- Request: Risks and Best Practices
- Digital Security Best Practices

Case Studies & Training Resources

- Case Study: Business Email Compromise
- Case Study: Account Takeover
- Case Study: Payment System Compromise