Cyber Security Landscape 2022
Andrew Morrison, Principal, US Leader Cyber Strategy
February 2022
ENTERPRISES CAN THRIVE IN AN ERA OF COMPLEXITY

- Digital interaction with clients and customers
- Leveraging the latest technological innovation
- Converging IT/OT and interconnecting supply chains
THE BUSINESS LANDSCAPE IS CHANGING AND LAUNCHING THE START OF THE 4\textsuperscript{TH} INDUSTRIAL REVOLUTION
The evolution of cyber risk is generally cumulative. That is, the drivers and opportunities in one era do not replace those of the preceding era. Rather, they expand the horizon. The era of compliance

- Chief Information Security Officers (CISOs)
- IT Risk Officers (ITROs)
- IT Risk assessment and strategy
- Large-scale risk and security program
- Development
- Identity and access management
- System implementation
- ERP security

The era of risk

- CISOs and ITROs
- Chief Risk Officers (CROs)
- Chief Information Officers (CIOs)
- CEOs, CFOs, CLOs and line-of-business leaders
- Boards of Directors
- Cyber Security
- Cyber Vigilance
- Cyber Resilience

The era of maturity and ubiquity

- CISOs, CIOs, ITROs, CROs, CEOs, CFOs, CLOs, LOB leaders, Boards
- Product managers and engineers
- Cyber-managed services
- Cloud-based cyber solutions
- Connected device security

In the wake of the Internet revolution, organizations focused on new standards for information security. The financial crisis also brought intensified focus on regulatory compliance in the areas of information and technology risk.

High-profile cyber attacks across multiple industries stimulated the attention of the media, the public, boards and executive management, inspiring many organizations to move beyond compliance examine the fundamental business risks of cyber.

Growing maturity across the capabilities and solutions of the past 15 years will drive many organizations to seek better cost efficiency. At the same time, the increasingly ubiquitous connectivity of products and infrastructure will intensify focus on managing risk in the Internet of Things.
SCALE, SOPHISTICATION AND IMPACT OF TODAY’S CYBER THREATS ARE INCREASING

Growing exploitation of our digital ecosystem
Threat actors moving with the age of digitalisation
Increasingly sustained and sophisticated attacks
MORE DETERMINED ACTORS OPERATING ON A GLOBAL SCALE

- Maximising options for opportunistic gain
- Shifting to direct targeting of internal networks
- Advancing social engineering and malware capability
Ransomware is the Most Prevalent Emerging Business Risk

Ransomware attacks now pose not only a cybersecurity risk, but also an enterprise-wide risk, threatening business continuity and operations. Through all the Deloitte Cyber Capabilities, different enterprise risks can be mitigated to build resiliency and fuel organization's preparedness when it comes to ransomware.

Why is Ransomware an Issue?


GROWING THREAT

4,000
Ransomware attacks occur daily

80% of Companies who paid the ransom experienced another attack

191 days
The average number of days an organization takes to identify a breach

80% increase
In the average number of cases that are exfiltrating and dropping ransomware

FINANCIAL TURMOIL

$265 BILLION
Ransomware attacks will cost its targets $265 billion by 2031

$350 M
Victims paid $350 million in ransom in 2020

104% increase
In the average ransom payment amount from Q4 2019

42%
42% of companies with cyber insurance did not have all losses covered by insurance

BUSINESS IMPACTS

19 days
The average time of system outages

92%
92% of companies who paid ransom do not get all their data restored

53%
53% of companies reported that their brand suffered

32%
32% of companies lost C-level talent as a direct result of a ransomware incident

26%
26% of organizations report a requirement to close operations for some period of time

The Anatomy of Ransomware

Before actively taking measure for preventing from a Ransomware attack, it is important to understand the overall lifecycle that takes place within an organization during an incident. Outlined below is the “anatomy” of ransomware and several industry specific examples.

### What Happens During a Ransomware Attack?

#### Reconnaissance
- Gathering and analyzing information to select vulnerabilities to enter the organization

#### Delivery
- Gaining access to organization’s networks and data through various entries (phishing, SQL inject, web)

#### Exploitation
- Installing backdoors, exploiting alternative vulnerabilities, and exfiltrating or destroying data

#### Impact
- Demand for Ransom and operational capabilities after recovery efforts

### Ransomware Industry Examples

**Reconnaissance**
- Identified a Virtual Private Network (VPN) without Multi Factor Authentication (MFA)
- Information was obtained through legitimate credentials used by attacker
- Exploited a zero-day vulnerability for VSA software access
- Purchased stolen credentials from an Initial Access Broker (IAB) and identified a lack of MFA

**Delivery**
- Utilized an inactive account credential to get initial access through a remote accessed network.
- Utilized a fake browser update from a legitimate website to inject malware
- Restricted admin access to prevent intervention and initiated malicious agent
- Accessed systems through stolen credentials to encrypt data

**Exploitation**
- Stole 100 gigabytes of data and caused a shut down of operations of necessary infrastructure
- Encrypted systems and ~75,000 client’s PII data alongside destroying backups
- Malicious update disabled malware prevention and related backups
- Encrypted and stole 150 gigabytes of data

**Impact**
- Paid $4.4 million to not have data leaked to attackers
- Paid $40 million to regain access to their network and decrypt client PII data
- Delayed patch development/restored, decryption key later received
- Paid $4.4 million to regain data access and prevent data disclosure

Sources: Bloomberg, EMIS, Heimdal Security, CSO Online, CSO Online, Heimdal Security, EMIS IT Governance UK
COMPLIANCE AND RESILIENCE IN A DIGITALLY-ENABLED WORLD

1. Getting the fundamentals right
2. Leveraging technology
3. Fusing capabilities
4. Having the right talent
GETTING THE FUNDAMENTALS RIGHT

Understand the criticality of your most important assets

Adopt a security posture relevant to your risk profile

Build a robust monitoring and response plan
OPPORTUNITY TO BETTER LEVERAGE TECHNOLOGY

- Adopt new solutions for faster detection and better prevention
- Leverage data to increase insight and visibility
- Exploit the digital opportunities of privacy
FUSING CAPABILITIES TO INCREASE VISIBILITY

Connect more to see more across the attack chain
Manage risk better, with less complexity and cost
Collaborate across industry to amplify effect

Cyber
Fraud
AML

Unified data and capability model

Data model
Threat intelligence
Control implementation
Scenario analysis
Response & investigation
Detection & analytics
Stress testing

Identify
Respond

Detect
Prevent
HAVING THE RIGHT TALENT

Deploy critical skill sets across regions and time zones
Build mixed teams of suits and hoodies
Grow and enable a new breed of cyber leaders
Deloitte & Touche LLP

Prefers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.nl/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 286,000 people make an impact that matters at www.deloitte.nl.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2019 Deloitte & Touche LLP