

CYBER RISK MANAGEMENT IN THE DIGITAL AGE



BDO DIGITAL CYBERSECURITY
SERVICES - March 2021

BDO DIGITAL

1

Cyber Risk Management Discussion Agenda

- The Cyber Risk Management Landscape
- Balancing Compliance and Security
- Managing Risk
- Assessing Cyber Risk Management Program Maturity
- Cyber Risk Management for the C-Suite & Board

2

BDO DIGITAL





2

1

THE CYBER RISK MANAGEMENT LANDSCAPE



EVOLUTION OF CYBER RISK MANAGEMENT LANDSCAPE

	 Risk Impact Potential	 Threat	 Motivation	 Capability
Then	<ul style="list-style-type: none"> Limited Internet Adoption; organization and government focus Initial e-commerce <p>► Potential Breach Impact = LOW</p>	<ul style="list-style-type: none"> Mainly Script Kiddies and underground hackers <p>► Threat Level = LOW</p>	<ul style="list-style-type: none"> Mainly Fame and Fun <p>► Motivation = LOW</p>	<ul style="list-style-type: none"> Basic capability widespread Advanced capability rare and specialized <p>► Impact of Capability = LOW</p>
Now	<ul style="list-style-type: none"> High Internet Adoption Advanced business and commerce Internet of Things <p>► Potential Breach Impact = MEDIUM/HIGH</p>	<ul style="list-style-type: none"> Cyber-criminal organizations Government funded operations <p>► Threat Level = HIGH</p>	<ul style="list-style-type: none"> Revenue Potential Acquiring Information Acquiring Intellectual Property <p>► Motivation = MEDIUM/HIGH</p>	<ul style="list-style-type: none"> Advanced capability common Tools published by hacker community require limited knowledge <p>► Impact of capability = MEDIUM/HIGH</p>

Source: Gregory Garrett, "Cyber Security in the Digital Age", Chapter 3 - "Information Security to Cyber Defense", New York: Wolters Kluwer 2018

Threat environment

- ▶ Significant increase in socially-engineered spear-phishing attacks using fake e-mails and fake websites, including:
 - Fake websites to sell protective equipment
 - Fake CDC information
 - COVID-19 Health Webinar - fake links
 - Fake government and healthcare reports
- ▶ Rise of ransomware attacks worldwide, especially targeting IOT connected devices
- ▶ Increased number of Business E-mail Compromise (BEC)/impersonation scams
- ▶ Growth of cyber-attacks on supply chains

“We are significantly dependent on information technology and our business may suffer from disruptions associated with information technology, cyber-attacks or other catastrophic losses affecting our IT infrastructure.”

Source: Alamo Group 2019 Annual Report

BDO DIGITAL

5

5

Threat environment example - common business e-mail scenarios

SCENARIO	DESCRIPTION
▶ Business Working with a Foreign Supplier	<ul style="list-style-type: none"> ▶ A business that typically has a longstanding relationship with a supplier is requested to wire funds for an invoice payment to an alternate, fraudulent account. ▶ The request may be made via telephone, fax, or e-mail. If an e-mail is received, the subject will spoof the e-mail request, so it appears like a legitimate request. ▶ Likewise, requests made via fax or phone call will closely mimic a legitimate request. This scenario has also been referred to as the “Bogus Invoice Scheme,” “Supplier Swindle,” and “Invoice Modification Scheme.”
▶ Business Executive Receiving or Initiating a Request for a Wire Transfer	<ul style="list-style-type: none"> ▶ The e-mail accounts of C-level business executives are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is typically responsible for processing these requests. ▶ In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank “X” for reason “Y.” This particular scenario has been referred to as “CEO Fraud,” “Business Executive Scam,” “Masquerading,” and “Financial Industry Wire Frauds.”
▶ Business Executive and Attorney Impersonation	<ul style="list-style-type: none"> ▶ Victims report being contacted by fraudsters who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. ▶ This type of BEC scam may occur at the end of the business day or work week and be timed to coincide with the close of business of international financial institutions.

BDO DIGITAL

6

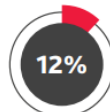
6

Bolstering Digital Resilience

The impact of COVID-19 has forced many organizations to make sudden changes, such as rapidly shifting to remote work, pivoting production or emphasizing digital revenue streams. The ability to leverage such changes is a key facet of business resilience. Repelling increased cyber threats is another crucial aspect of resilience. While emerging technologies have helped streamline and optimize many different processes, they also expose businesses to significant risk. There has never been more information to harness and to simultaneously insulate from risk. Because of the grave consequences of data mismanagement and exposure, data privacy and security risks are top of mind for middle market executives.



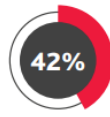
39% cite cyber attacks as their #1 digital threat



12% of CFOs cite data privacy as their #1 overall business priority



59% say bolstering cybersecurity is one of their top 3 short-term business goals (12-18 months)
 ▶ 40% say bolstering cybersecurity is one of their top 3 long-term business goals (18 months-3 years)



42% are planning digital initiatives in the area of risk management and compliance over the next 12 months
 ▶ 46% already have projects underway

7

Source: Building Tomorrow's Business: How the Middle Market is Tackling Disruption Today / 2020 BDO Digital Transformation Survey
 600 C-Suite Executives were surveyed from companies ranging from annual revenues of \$250 million and \$3 billion.



7

DATA BREACH METRICS

52%

caused by malicious or criminal attacks

\$3.86 million

average cost of a data breach globally

-1.5% versus 2019 (\$3.92 million)

\$8.64 million

Average cost of a U.S. data breach

Canada - \$4.5 M, France - \$4.01 M, UK - \$3.9 M

76%

of companies predict that remote work will make breach response more difficult

80%

of breaches exposed customer PII

\$150

per customer PII record cost

DOES YOUR ORGANIZATION FACTOR IN DATA BREACH AND RELATED COSTS INTO THE BUDGET?

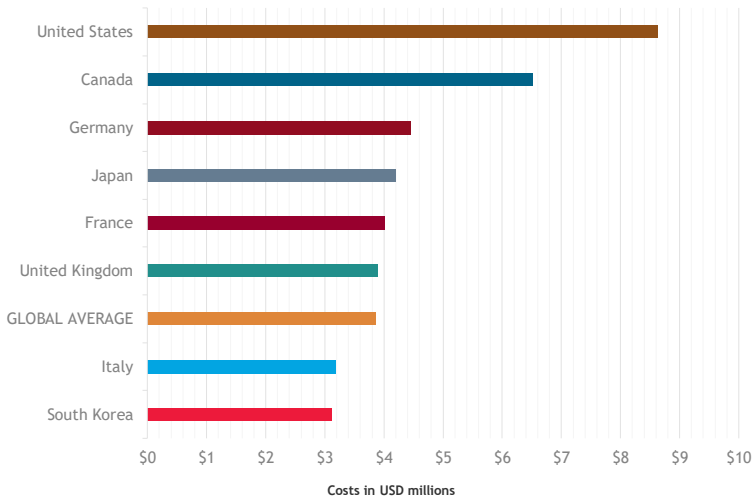
8

Source: Cost of a Data Breach Report, IBM, 2020



8

DATA BREACH COSTS BY COUNTRY



9

Source: IBM Security Report - 2020

While the global average cost of a data breach is \$3.86 million, the cost by country varies.

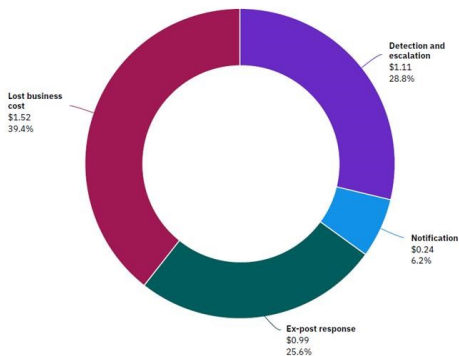
Despite the average cost of a data breach declining by 1.5% between 2019 and 2020 across global jurisdictions, the cost of a data breach in the United States continues to exceed other countries at \$8.64 million.

BDO DIGITAL

9

COMPONENTS OF DATA BREACH COST

Data breach average total cost divided into four categories
Measured in US\$ millions



► Based on global averages, the four cost segments in U.S. dollars and percentage of the total cost of a data breach are:

- Lost Business
- Detection and escalation
- Ex-post response
- Notification

► Lost business cost an average of \$1.52 million or 39% of total cost.

► The lowest cost was for notification of the data breach, at \$240,000 or 6% of total cost.

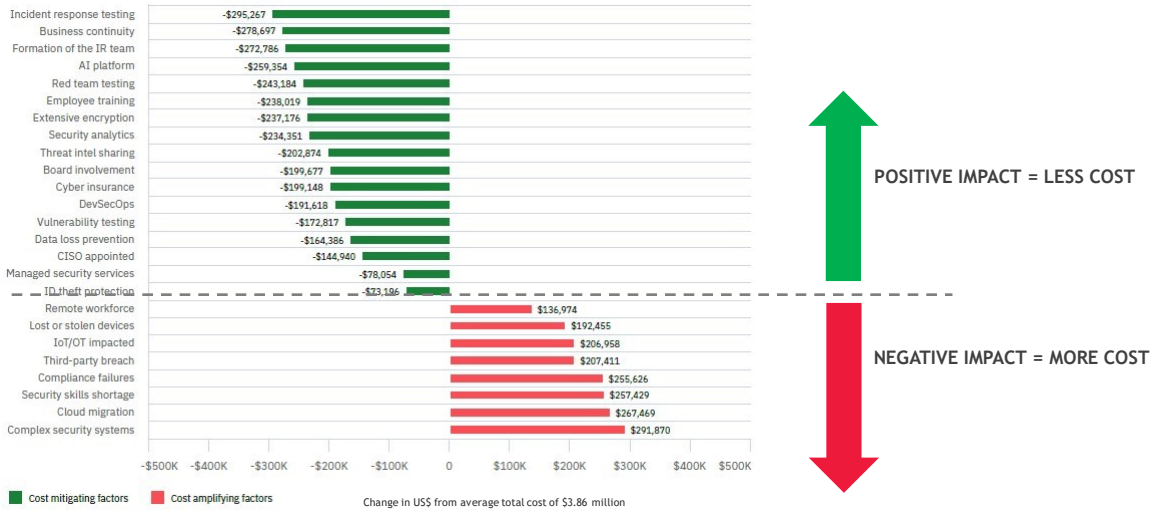
10

Source: Cost of a Data Breach Report, IBM, 2020

BDO DIGITAL

10

IMPACT OF FACTORS ON COST OF DATA BREACH



11

Source: Cost of a Data Breach Report, IBM, 2020



11

REGULATORY CONSIDERATIONS

EUROPE

- ▶ European Data Protection Board - crisis data processing
- ▶ European Union Regulators - pandemic impact on privacy
- ▶ European Parliament Civil Liberties Committee Chair - contact tracing apps must respect privacy

CANADA

- ▶ Issued guidance for organizations to manage federal privacy laws

UNITED STATES

- ▶ CCPA enforcement - 7/1, CPRA - ballot, 11/20
- ▶ AZ - AG suit against Google (deceptive trade)
- ▶ NJ - consumer opt-in and notification updates
- ▶ NY, NJ, CT - tri-state contact tracing bill

CHINA

- ▶ Wuhan - Government Surveillance to enter region



12

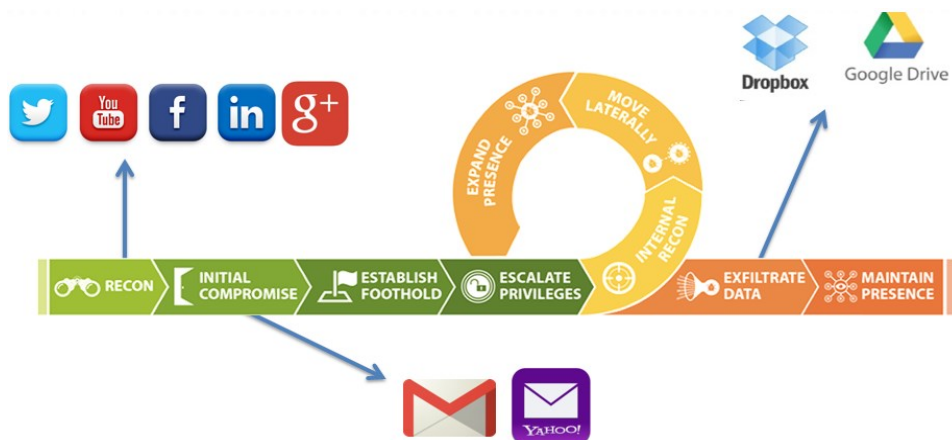


12

COMPONENTS OF A CYBER BREACH



STAGES OF A CYBER DATA BREACH



TOP CYBER RISK MANAGEMENT TRENDS

- ▶ Blurring of cyber - threat actors
- ▶ Rise of Business E-mail Compromise (BEC)
- ▶ Growth of spear-phishing e-mail attacks (up 70%)
- ▶ Expansion of ransomware attacks (up 350%)
- ▶ Exploitation of supply chain network attacks
- ▶ Greater U.S. Securities & Exchange Commission (SEC) focus on cybersecurity
- ▶ Increasingly complex regulatory landscape
- ▶ Shortage of experienced cybersecurity and data protection talent
- ▶ Onset of cyber attack fatigue/burn-out factor
- ▶ Risks imposed by remote workplace



FREQUENTLY ASKED QUESTIONS ABOUT CYBERSECURITY

- ▶ What should I know about cybersecurity?
- ▶ Does our organization understand what is at stake?
- ▶ What should I do about cybersecurity?
- ▶ How should I assess the quality of my organization's cybersecurity program? How likely are we to be a victim of a cybercrime?
- ▶ How can we put cybersecurity and data protection first?
- ▶ What threats are facing our company?
- ▶ What Cloud services does our organization use and how risky are they?
- ▶ How are we protecting sensitive data?
- ▶ Should we train all professionals on cybersecurity and protecting sensitive data?

BALANCING COMPLIANCE AND SECURITY



17

BALANCING COMPLIANCE AND SECURITY

What is Security?
Security is the unique ecosystem of policies, processes, and technical controls that define how an institution effectively protects data from cyber threats.

Contrary to changing slowly and predictably like the compliance landscape, the security/threat landscape

- ▶ is in a perpetual state of change,
- ▶ is not meant to satisfy a third party's needs and
- ▶ is driven by the need to protect against constant threats to an organization's assets and is never finished but is continuously maintained and improved.

Since there is considerable overlap in being compliant with being secure, in a perfect world organizations would just do both. However, in reality every institution has limitations in available resources, whether from the perspective of qualified personnel or adequate funding. This creates the need to prioritize and identify trade-offs.



18

BALANCING COMPLIANCE AND SECURITY

Addressing compliance will never be simple for organizations. There are things which can be done to help simplify the task. Let's discuss a few of these:



Have Clear, Achievable Policies



Conduct an Organizational Cyber Risk Assessment



Define What Is Necessary for Compliance



Be Transparent With Your Regulators



Find a Balance



Avoid a Checklist Approach



Take a Managing Risk Approach

19

BDO DIGITAL

19

MANAGING RISK



BDO DIGITAL

20

10

MANAGING RISK - UNDERSTANDING RISK

- ▶ What is my risk tolerance?
 - ▶ Define Organizational Risk Tolerance
 - ▶ Determine the tolerance (from high to low) for various impact categories (e.g., financial, operational, regulatory, etc.).
- ▶ What are my 'Crown Jewels'?
 - ▶ Identify Assets and Crown Jewels
 - ▶ Determine the key business processes (e.g., product development) and potential crown jewels (e.g., critical systems and related data) that organization relies on.
 - ▶ For each assess the confidentiality, integrity, and availability impacts to determine the specific risk levels.
- ▶ What are my threats?
 - ▶ Identify and Assess Threats
 - ▶ Identify relevant threat actors (e.g., adversarial, accidental, environmental) that could have a negative impact on organization.
 - ▶ Identify key threat scenarios applicable to organization and map key expected controls for their mitigation.



21

21

MANAGING RISK - MITIGATING RISK

- ▶ How strong are my controls?
 - ▶ Evaluate Capabilities
 - ▶ Assess the state of controls across the organization for protecting against identified threats
- ▶ What are my residual risk areas and what to do next?
 - ▶ Calculate Risk and Define Remediation Activities
 - ▶ Based on threat assessment (likelihood) and assets evaluation (impact), calculate the inherent and residual risk.
 - ▶ Evaluate residual risk against organization's risk tolerance



22

22

TAKING A RISK MANAGEMENT APPROACH



23

BDO DIGITAL

23

MANAGING CYBER RISK - A SUMMARY

- What is commonly referred to as Cybersecurity is an evolution of Information Security in the context of an organization's risk management program.
- Cybersecurity needs to be managed consistently with other risk disciplines.
- Core to any cybersecurity program is confidentiality, integrity, and availability.
- Cyber risk management also encompasses principles to defend your reputation, finances, and at times life threatening situations.



24

BDO DIGITAL

24

ASSESSING CYBER RISK MANAGEMENT PROGRAM MATURITY



25

CYBER RISK MANAGEMENT MATURITY

Cybersecurity maturity, used as a performance metric, offers additional insight into how the security organization is operating. It can be used to analyze compliance and operational data at the process or function level. Trends can be discovered, monitored and adjusted for.



26

BDO DIGITAL

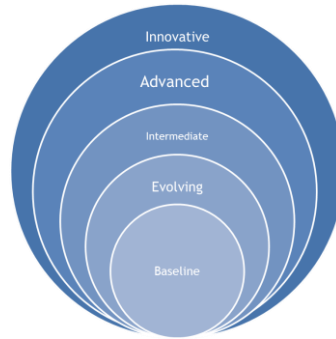
26

CYBER RISK MANAGEMENT MATURITY SAMPLE OVERVIEW

Cybersecurity maturity is often expressed in five domains:

- Domain 1 - Cyber Risk Management and Oversight,
- Domain 2 - Threat Intelligence and Collaboration,
- Domain 3 - Cybersecurity Controls,
- Domain 4 - External Dependency Management,
- Domain 5 - Cyber Incident Management and Resilience.

Each domain has five levels of maturity: baseline, evolving, intermediate, advanced, and innovative.



Source: FFIEC Cybersecurity Assessment Tool

CYBER RISK MANAGEMENT MATURITY: WHAT MAKES SENSE?

A cyber risk management program should be scalable and scoped based on: size and complexity of the entity, nature and scope of the activities of the entity, sensitivity of the information to be protected, cost and availability of tools to improve, and resources available to the covered entity.

		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				■	■
	Advanced			■	■	■
	Intermediate		■	■	■	
	Evolving	■	■	■		
	Baseline	■	■			

Source: FFIEC Cybersecurity Assessment Tool

CYBER RISK MANAGEMENT FOR THE C-SUITE & BOARD



29

CYBER RISK MANAGEMENT FOR THE C-SUITE & BOARD

The cybersecurity market has grown rapidly, offering a wide range of cybersecurity hardware, software and professional services. There are many companies offering cybersecurity products and services, often claiming to have a one-stop solution to your cybersecurity needs. However, executives and the Board should recognize that:

- ▶ There is no single product or service that can provide a magical solution
- ▶ Cybersecurity is multi-faceted and highly-complex
- ▶ Data protection is no longer a regional issue, rather it's a global challenge.

Executives are trying to make the right investment decisions but are not always well informed regarding the cyber threats, and potential cyber liabilities, facing their organization. Rather than investing valuable resources in protecting specific types of high-value data, a threat-based approach to cybersecurity identifies the vulnerabilities that a cyber attack would likely try to exploit, and outlines measures to secure those vulnerabilities.



30

BDO DIGITAL

30

TOP FIVE THINGS CEOS SHOULD KNOW ABOUT CYBER RISK

- ▶ Cyber attacks and security breaches will occur and will negatively impact the business
- ▶ According to most cybersecurity surveys, over 60% of all data breaches originate from unauthorized access from one of the organization's current or former employees, or third-party suppliers
- ▶ Achieving information security compliance with one or more government regulatory standard for information security (i.e., ISO 27001, NIST 800-171, HIPAA, NYDFS, etc.) is good, but not sufficient to holistically address cybersecurity
- ▶ Cyber liability insurance premiums are significantly increasing in cost and often do not cover all the damages caused by a cyber breach
- ▶ To achieve real information security and data resilience, it is vital to combine managed Monitoring, Detection, and Response (MDR) Managed Security Services (MSS) with comprehensive disaster recovery (DR) and business continuity plans (BCP)

CYBER LIABILITY INSURANCE CONSIDERATIONS

- ▶ A cyber insurance policy protects against first-party and third-party loss.
- ▶ First party loss is considered an interruption, damage, or destruction to your or dependent providers' property, resulting in property damage, business interruption, and associated costs.
- ▶ Third-party loss is bodily, personal, or property damage a cyber event causes to others due to your actions or inactions.
- ▶ This exposure includes privacy liability, fines and penalties, and other associated injuries.
- ▶ Items often not covered; sales loss, 3rd party mistakes, new hardware, software upgrades, and PCI fines. In addition many policies include a "waiting period" before coverage kicks in.

31

Source: Building Tomorrow's Business: How the Middle Market is Tackling Disruption Today / 2020 BDO Digital Transformation Survey
600 C-Suite Executives were surveyed from companies ranging from annual revenues of \$250 million and \$3 billion.



31

TOP TEN THINGS CEOS SHOULD DO ABOUT CYBER RISK

1. Ensure everyone in the organization from the top-down receives appropriate cybersecurity education and awareness training.
2. Hire an independent company to conduct a cyber risk assessment to identify potential gaps in the organization's information security policies, processes, plans, and procedures.
3. Verify that periodic penetration testing by certified Ethical Hackers is being conducted to identify potential cybersecurity vulnerabilities in the organization's information systems.
4. Require a timely and effective software patch management program be implemented by the organization's Information Technology team to mitigate known security vulnerabilities as quickly as possible.
5. Ensure the organization has 24 x 7 x 365 monitoring, detection, and response capabilities for its information systems.
6. Verify the organization has an appropriate cyber breach incident response plan, including the policy and procedures related to ransomware attacks.
7. Hire an independent firm to conduct a cyber liability insurance coverage adequacy evaluation.
8. Establish information security key performance indicators (i.e. number of cyber-attacks, number of data breaches, network uptime, network downtime, cost of cyber breaches, cost of cyber insurance, cost of information security as a percentage of total company IT cost, etc.).
9. Ensure the organization has well-documented and periodically tested disaster recovery and business continuity plans to quickly recover lost or stolen data to mitigate potential damages of cyber breaches.
10. Mandate additional layers of information security via encryption, multi-factor authentication, and highly restricted access to the organization's most valuable information assets.

32

Sources: Gregory Garrett, "Cyber Security in the Digital Age", Chapter 2 - "Cybersecurity for the C-Suite & Board", New York: Wolters Kluwer 2018



32

SEVEN STRATEGIC QUESTIONS A CEO SHOULD ASK



- ▶ What is the threat profile of our organization based on our business model and the type of data our organization holds?
- ▶ Who may be after our organization's data assets - Nation States, sophisticated international criminal organizations, ideologically motivated hackers, competitors in the market, disgruntled former employees?
- ▶ Does our organization's cybersecurity strategy align with our threat profile?
- ▶ Is our cybersecurity risk viewed as an enterprise-wide issue and incorporated into our overall risk identification, management and mitigation process?
- ▶ What percentage of our IT budget is dedicated to cybersecurity? Does that allocation conform to industry standards? Is it adequate based on our threat profile?
- ▶ Is there someone dedicated full-time to our cybersecurity mission and function, such as a Chief Information Security Officer (CISO)?
- ▶ Is our cybersecurity function properly aligned within the organization?
(Aligning the CISO under the CIO may not always be the best model as it may present a conflict. Many organizations align this function under the risk, compliance, audit or legal functions - some with direct or "dotted line" reporting to the CEO.)

33

www.bdo.com/digital



BDO DIGITAL

33

QUESTIONS & ANSWERS



BDO DIGITAL

34