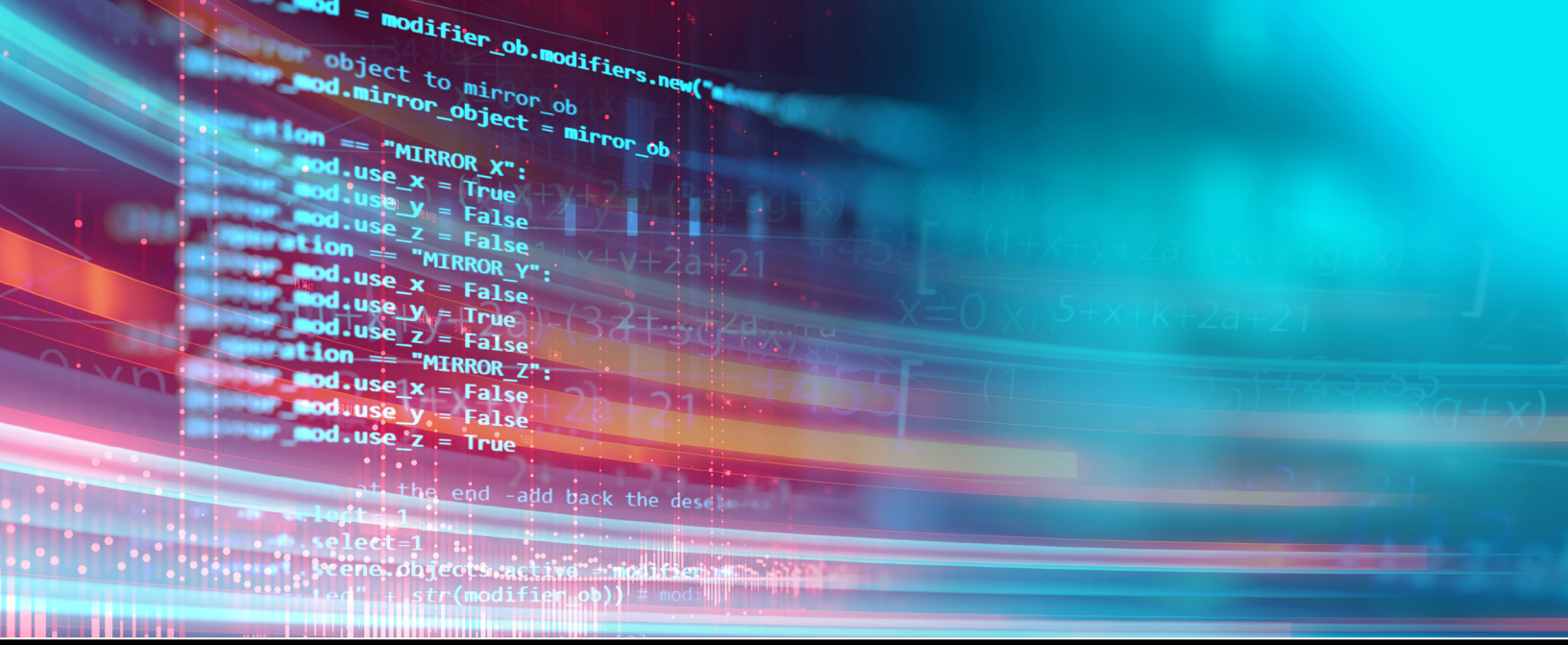


Cyber & Technology Practice Playbook

Part I: Common Adversary Attacks

A practical guide for executives to navigate best practices in cyber risk management

LOCKTON®

Cyber facts

7.7B
WORLD POPULATION[1]

2.5B
MOBILE SUBSCRIBERS[2]

$3.5B
COST OF CYBERCRIME IN 2019 (AS REPORTED TO THE FBI'S INTERNET CRIME COMPLAINT CENTER (IC3))

ESTIMATES ARE THAT ONLY
10%-12%
OF CYBERCRIME INCIDENTS ARE REPORTED TO IC3

$5.2T
COST OF CYBERCRIME BY 2025[4]

$3.92M
AVERAGE COST OF DATA BREACH[5]

1.2B
PREDICTED INCREASE IN INTERNET USERS FROM 2019 TO 2025[6]

25,575 RECORDS
AVERAGE SIZE OF A DATA BREACH[7]

279 DAYS
AVERAGE LIFE CYCLE OF A BREACH[8]

43%
OF BREACHES AFFECT SMALL BUSINESS VICTIMS[9]

49%
OF C-LEVEL EXECUTIVES HAVE CYBERSECURITY ISSUES ON QUARTERLY BOARD AGENDAS[10]

4%
OF C-LEVEL EXECUTIVES HAVE CYBERSECURITY ON MONTHLY BOARD AGENDAS[11]

Standardized guidelines & best practices

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CREATED A VOLUNTARY FRAMEWORK consisting of standard guidelines and best practices to address cybersecurity risks. The five pillars represent a holistic approach to cybersecurity.[17] The Cybersecurity and Infrastructure Security Agency (CISA) explains and summarizes the framework's five function areas.[18]

INCREASED REGULATIONS & ENFORCEMENT

"The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected — with relatively little built-in security — and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits."[12]

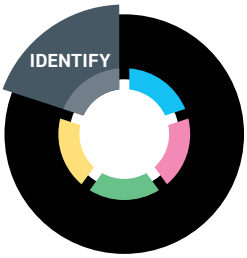
"Cybersecurity risks pose grave threats to investors, our capital markets and our country."[13]

The €50M fine imposed on Google was, "justified by the severity of the infringements observed regarding the essential principles of the GDPR: transparency, information and consent."[14]

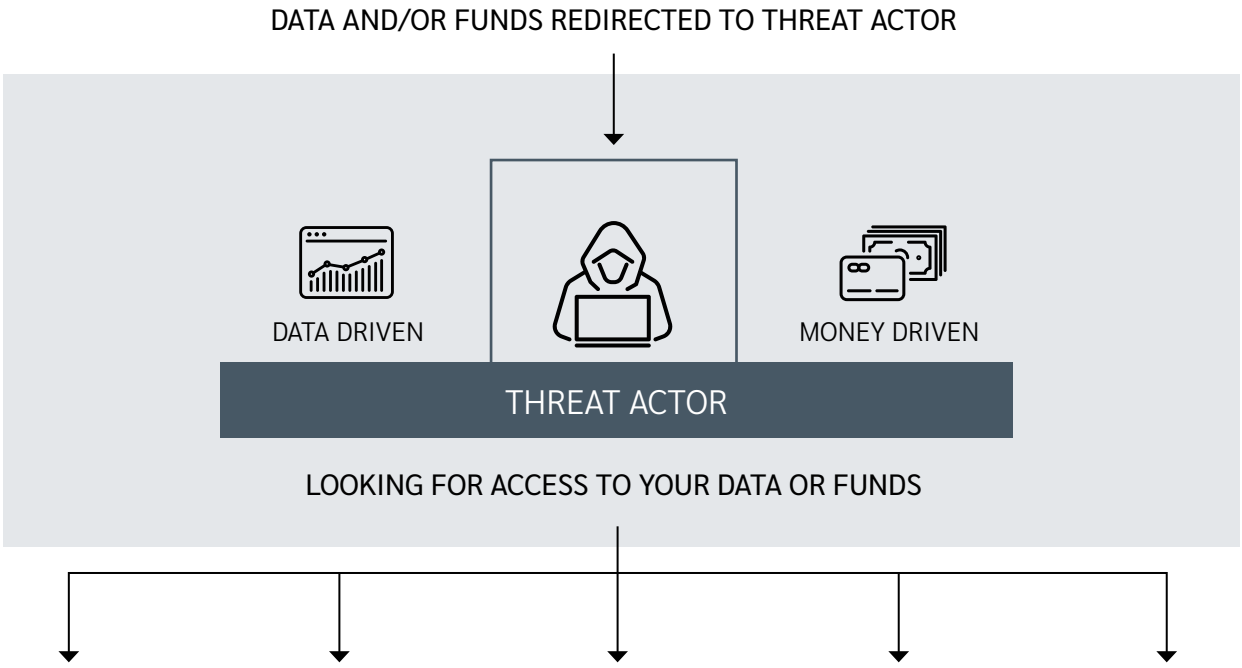
"The magnitude of the $5B penalty and sweeping conduct relief are unprecedented in the history of the FTC. The relief is designed not only to punish future violations but, more importantly, to change Facebook's entire privacy culture to decrease the likelihood of continued violations. The Commission takes consumer privacy seriously, and will enforce FTC orders to the fullest extent of the law."[15]

"HIPAA compliance depends on accurate and timely self-reporting of breaches because patients and the public have a right to know when sensitive information has been exposed. When health care providers blatantly fail to report breaches as required by law, they should expect vigorous enforcement action by OCR."[16]

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event



Cyber vulnerability



MALICIOUS MESSAGES

The threat actor uses deceptive emails, texts and phone calls/ messages to mislead the target into believing that the sender is legitimate.

COMPROMISED CREDENTIALS

The threat actor may obtain compromised credentials from the dark web and/ or make minor modifications to weak or reused credentials.

OUTDATED SYSTEM

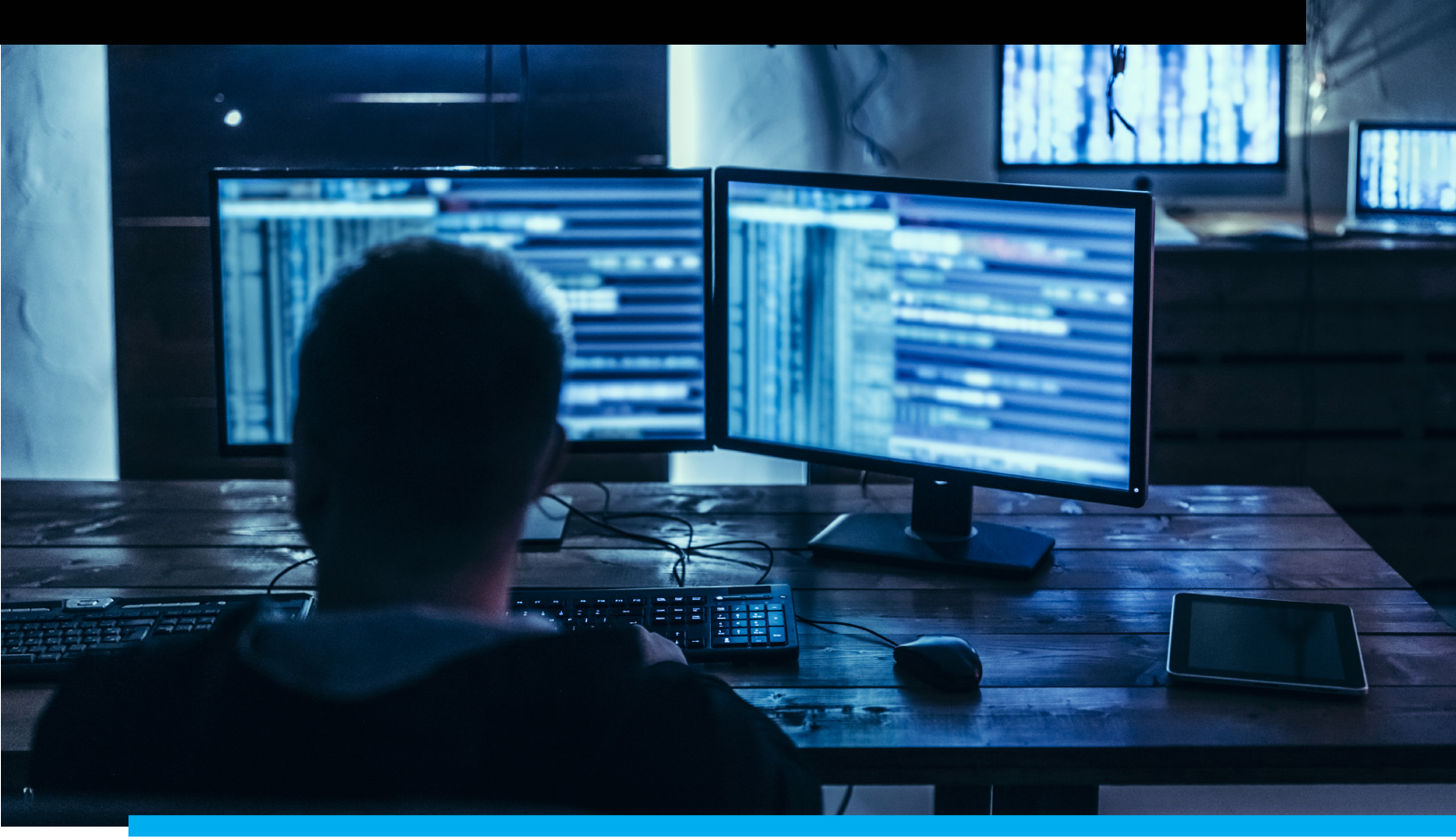
Failure to update hardware and software creates vulnerabilities, giving the threat actor opportunities to access data and/ or funds.

ONLINE EAVESDROPPING

The threat actor prowls unsecured Internet usage and shadows the target to access data and/ or funds.

SECURITY WEAKNESS

Network and website misconfiguration, unencrypted devices, and missed patches are prime opportunities for access by the threat actor.



Common cyberattacks

MALWARE	SOCIAL ENGINEERING	MAN-IN-THE MIDDLE	DENIAL OF SERVICE	SQL INJECTION
Spyware	Phishing	Email hijacking	Denial-of-service attack	
Ransomware	Spear phishing	Wi-Fi and browser eavesdropping	Distributed denial of service	
Worms	Whaling	IP and DNS spoofing		
Trojan horses	Vishing			
	Baiting			
	Pretexting			
	Tailgating/ piggybacking			
	Quid pro quo			

What you can do to safeguard

Employee training and awareness	Limit access to confidential and sensitive data
Strong passwords	Secure networks
Multi-factor authentication	Update hardware and software
Develop written security policies and protocols, including an incident response plan	Regular backups not connected to network

Cybersecurity & corporate governance

SAMPLE AGENDA ITEMS FOR THE BOARD

- What is our cybersecurity strategy?
- What cyber risks impact our clients, people, operations and reputation, and what is our plan to deal with them?
- Have we quantified the financial impact?
- Does our business continuity plan contemplate cyber and technology risks?
- What is our local, state, federal and international cybersecurity compliance strategy?
- Is there sufficient cyber/technology expertise represented on the board?
- Who are the key players necessary to create and implement the cybersecurity strategy?
- Who is ultimately responsible?
- Do we have an incident plan in place and how often is it reviewed and updated?
- What is our communication strategy for incident response and compliance?
- Do we have sufficient risk transfer mechanisms in place (insurance and contractual indemnity)?
- What are our protocols for reviewing third-party vendors' contracts and cybersecurity procedures?

What happens when there is an incident?

PROCESS BEGINS UPON receipt of a regulatory inquiry, written demand, arbitration demand, and/or complaint OR notice of breach, suspected breach, suspicious activity on the network, security incident and/or ransomware attack.

START

STEP 1

CONTACT

Client notifies Lockton of incident.
Lockton provides client with insurer panel list and provides notice of incident to insurer(s).

*Review and select counsel from insurer's preapproved panel. With first-party incident, counsel will serve as breach coach and help determine scope and breadth of incident.**

STEP 2

INVESTIGATE

Insurer acknowledges claim and begins investigation into policy and facts to determine coverage.

Collaborate with breach counsel to select and retain appropriate team to assist, e.g., forensics firm, IT consultants, ransom negotiator and/or public relations firm.

*ADDITIONAL INFORMATION

DEFENSE OBLIGATIONS

- **Duty to defend policy:** Insurer selects attorney to defend your interests.
- **Reimbursement policy:** Insured selects counsel but must seek consent to firm and rates.

PANEL LIST BENEFITS

- Expertise in cybersecurity and privacy liability
- Knowledge of your insurer's guidelines, reporting requirements and approval/consent procedures
- Prenegotiated rates not available if engaged outside the insurance relationship

SAMPLE INCIDENTS

FIRST-PARTY SCENARIOS

- Breach or suspected breach incident
- Suspicious activity on network
- Security incident
- Ransomware attack

THIRD-PARTY SCENARIOS

- Regulatory inquiry
- Third-party demand and/or claim
- Complaint
- Demand for arbitration

If necessary, provide the notifications to affected individuals, regulators, law enforcement.

FINISH

STEP 3

MITIGATE

Insurer engages with insured and breach counsel regarding necessary steps to minimize the insured's exposures.

STEP 4

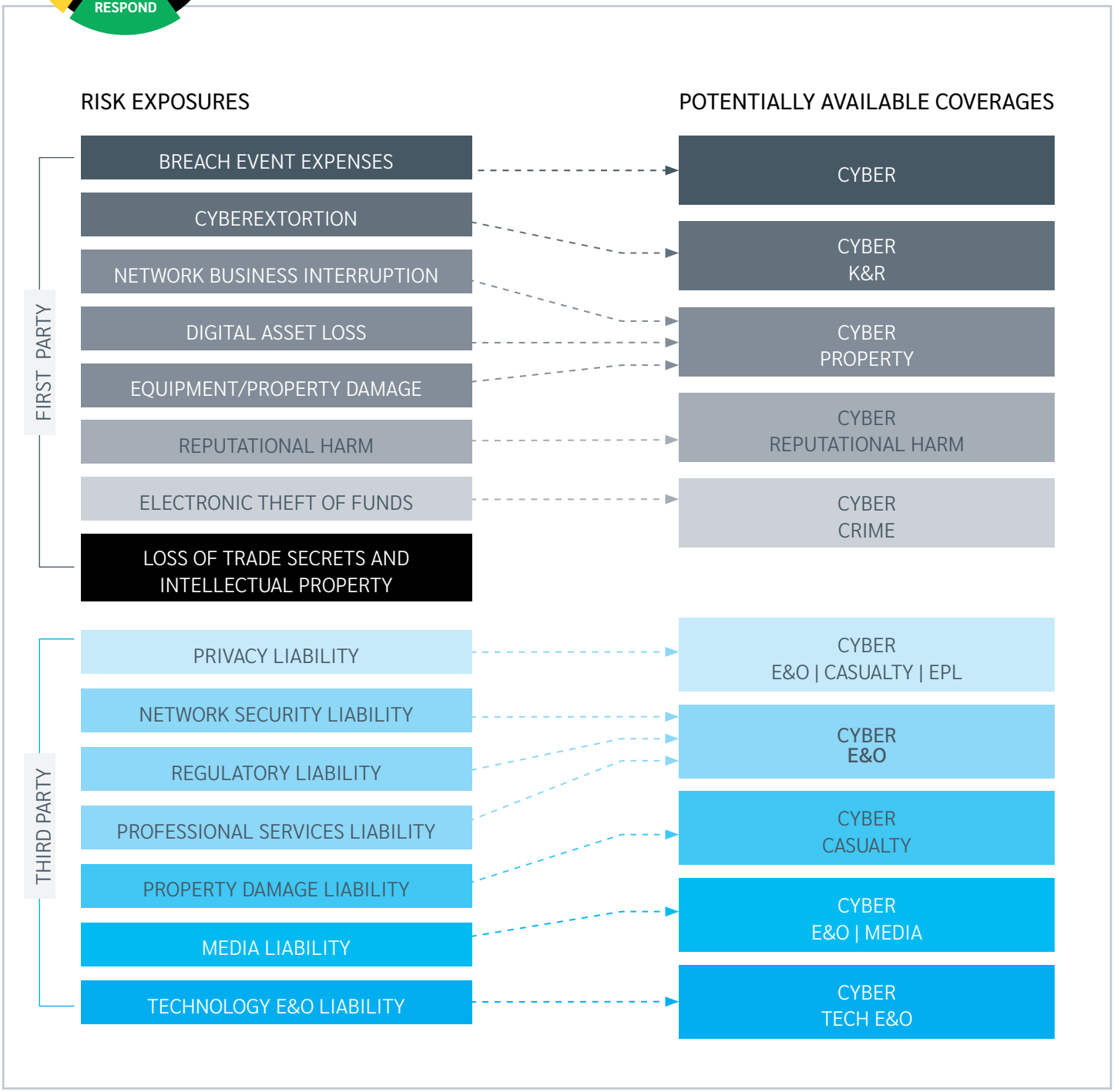
REMEDIATE

Insurer reviews proposed remediation measures to determine scope of coverage afforded for the remediation efforts.

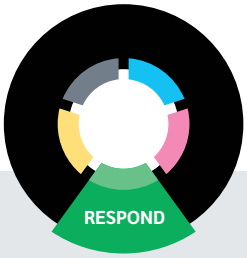
POST-INCIDENT CONSIDERATIONS

- Forensic accounting services to assist in quantifying the business interruption losses
- Internal and external threat and vulnerability assessments and improvements
- Incident response assessment and improvement
- Education and training of employees and leadership
- Policies and procedures review and improvement

Insurance & risk transfer



Sample incidents



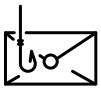
Malware

An email purporting to be from your client is sent to one of your project managers, who clicks on the link. Unknown to your project manager or anyone else at your organization, the threat actor installs malware onto your systems. Your project manager thinks nothing of it and deletes the email. Everyone goes back to business and work routines. Four months later, you come into the office and try to turn on your computer, and there is a message stating that your computer has been locked and you will need to pay $575,000 to obtain the encryption keys.

FACTORS TO CONSIDER

- How to get back up and operational?
- What happened to cause the incident?
- What are the notification obligations, if any?
- Should this be reported to law enforcement?
- How much are your business interruption losses?
- What are the potential liability exposures of the company?

Social engineering



An email purporting to be from your CEO is sent to your accounting department requesting that all your employees' W-2s be sent to the CEO immediately. The accounting clerk sends an email back to the threat actor purporting to be the CEO, attaching all your employees' W-2s.

FACTORS TO CONSIDER

- What happened?
- What steps are necessary to contain the incident?
- What steps are necessary to mitigate the incident?
- What are the notification obligations, if any?
- What are the potential liability exposures of the company because of the incident?

Physical theft

Your company issues laptops to your employees so that they can work remotely ,with clear instructions that no work materials should be saved on the desktop. Your employee is working on an important project and, to save time, stores several client health records on the desktop. After a long day working on the project, your employee goes out to dinner and leaves the laptop in the back seat of the car. The car is broken into, and the laptop is stolen.

FACTORS TO CONSIDER

- Is the laptop encrypted?
- Is there the ability to wipe the laptop remotely?
- What information on the laptop is potentially accessible by a threat actor?
- What are the notification obligations, if any?
- Has a police report been filed?
- What are the potential liability exposures of the company because of the incident?

Understanding your cyber risk

A sound cyber risk management plan protects your balance sheet, preserves your reputation and enables growth in your organization. That's exactly what our three-step approach is designed to accomplish.

First, your trusted advisor will inform you of exposures, risks and financial impact, supported by next-generation analytics.

Then, our loss control and risk consulting services are available to ensure our team is helping to constantly improve your cyber climate. Deep-seated relationships with insurance companies and strategic partnerships with security firms offer an extra layer of support.

Finally, we'll design and tailor your insurance program and risk transfer strategies to fit your unique needs.

This coordinated three-step approach ensures that you thoroughly understand your exposures and are supported, prepared and equipped with the best cyber risk protection plan for your organization.

Lockton's three-step approach: Inform, Improve, & Insure

NAVIGATING THE BEST CYBERSECURITY SOLUTION PROVIDERS CAN BE OVERWHELMING. That's why you'll be paired with a trusted advisor, who's equipped to lead you through the process.

Inform

ANALYSIS

- Insurance program benchmarking
- Coverage gap analysis
- Data on thousands of insurance programs

ASSESSMENT

- Cyber risk posture and maturity
- External vulnerability scan

QUANTIFICATION

- Data breach
- Business interruption
- Dynamic Capital Modeling
- Bespoke modeling

Improve

LOSS CONTROL

- Cyber risk reviews
- Incident response exercises

RISK CONSULTING

- Data breach scenarios
- Board/executive education and engagement

PARTNERED SERVICES

- Managed detection and response
- Forensic accounting
- Data landscaping
- And more

Insure

TAILORED INSURANCE SOLUTIONS

- Comprehensive risk protection programs with property, casualty, D&O, crime, and more
- Policies crafted to address each client's unique risks

MARKET COVERAGE

- Global carrier relationships and broader coverage provide clients with more options
- Proprietary forms
- Enhancement endorsements

CLAIMS ADVOCACY

- Experienced and forceful advocacy with insurers
- Use claim experience to constantly improve policy language
- Claims administration and support

Lockton Global Cyber & Technology team

AS THE WORLD'S LARGEST PRIVATELY OWNED, INDEPENDENT INSURANCE BROKER. Lockton's independence gives us the freedom to be a strong, flexible advocate always acting in the best interest of our clients, creating an entirely different dynamic — one that's focused on your success. Led by a premier team of cyber brokers and advisors, Lockton's Global Cyber & Technology team is dedicated to delivering unparalleled service and innovative programs for your organizational needs.

Supported by cyber claims experts, former security practitioners and legally qualified technicians, our global team offers a wide range of expertise in risk identification, protection and management, as well as proven delivery of results.

Our global reach ensures that our clients have access to the knowledge that comes from experiences across multiple jurisdictions and multiple industries.

Unmatched insurance and risk transfer program advisory and placement solutions:

50+ Cyber & Technology Associates globally

More than 300 incidents handled each year with a 99% covered claim rate to date

Relationships with more than 175 insurance companies globally

Asia

BANGKOK

Viyada Engchuan

Rob Russell

HONG KONG

Calvin Kwan

Rory Young

SINGAPORE

Frederic Boles

Australia

SYDNEY

Mark Luckin

Bermuda

Phil DiMeglio

Mexico

MEXICO CITY

Karla Castro

Norway

OSLO

Anders Smedsrod

Middle East/ North Africa

DUBAI

Zainab Khatib

United Kingdom

LONDON

Carl Moore

Lucy Scott

Vanessa Cathie

Mark Walters

Liam Brown

Reece Kent

James Harris

Teddy King

Peter Erceg

Alicia King

Carlo Ramadoro

Brett Warburton-Smith

Sebastian Legget

Will Moore

Luke Morenas-Jones

Kajal Desor

United States

CHARLOTTE

Grady Kellogg

CHICAGO

Matt McAleenan

Riley Brant

DALLAS

Peter Smith

Ashley Jones

DENVER

Tim Smit

Kit Cabonor

KANSAS CITY

Bill Boeck

India Foss

Tom Howell

Madeline Allen

Evan Miller

Kevin Gunya

Nathan Waddell

Tyler Klein

LOS ANGELES

Chris Reese

Sarah Windsor

Maryam Rad

Taylor Bennett

Brian Moffitt

Hannah Hays

Leigh Tuccio

Matthew Leyva

Katia Gilbon Morales

NEW YORK

Anthony Dagostino

Ryan Gibney

David Anderson

Grady Martin

Imani Barnes

Beth Gidicsin

Alex Leone

SAN FRANCISCO

Brian Pfund

Emily Boody

WASHINGTON, DC

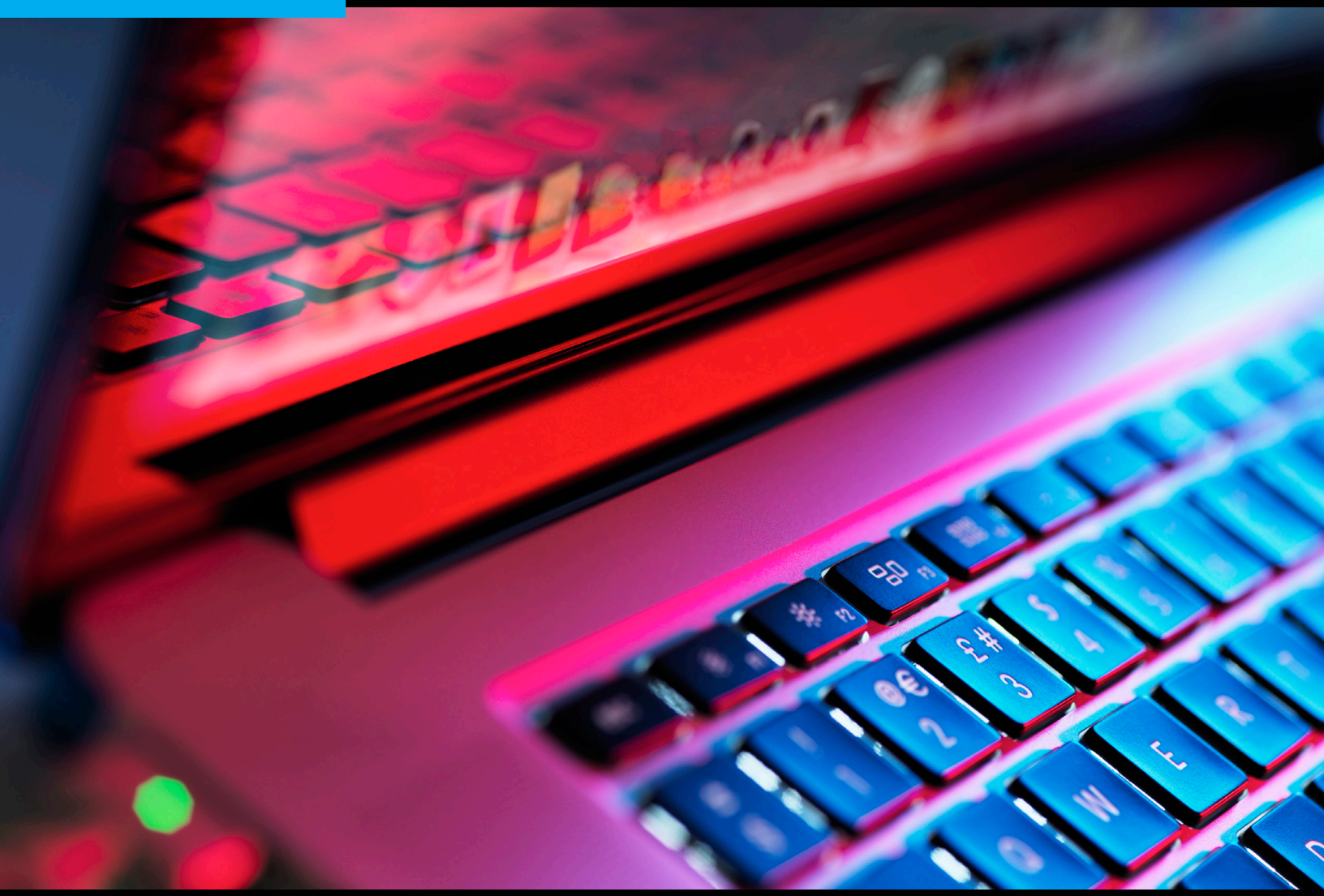
Caroline Chapman

Tim Monahan

Colin White

Hunter Stoycos

CONTACT THE LOCKTON CYBER & TECHNOLOGY PRACTICE AT CYBER@LOCKTON.COM.



Sources

[1] https://population.un.org/wpp/Publications/Files/WPP2019_Highlights.pdf

[2] www.gsma.com/mobileeconomy/

[3] https://pdf.ic3.gov/2019_IC3Report.pdf

[4] www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

[5] www.ibm.com/security/data-breach

[6] www.gsma.com/mobileeconomy/

[7] www.ibm.com/security/data-breach

[8] www.newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

[9] www.enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/

[10] www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf

[11] www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-the-future-of-cyber-survey.pdf

[12] www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

[13] www.sec.gov/rules/interp/2018/33-10459.pdf

[14] www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

[15] www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

[16] www.hhs.gov/about/news/2019/11/27/ocr-secures-2.175-million-dollars-hipaa-settlement-breach-notification-and-privacy-rules.html

[17] www.nist.gov/cyberframework/online-learning/five-functions

[18] www.us-cert.gov/resources/cybersecurity-framework

Notes

UNCOMMONLY INDEPENDENT