BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

Ransomware Preparation and Incident Response

SESSION: March 7, 9 am – 3 pm
Analyst: Michel Hebert, PhD
mhebert@infotech.com

INFO~TECH RESEARCH GROUP

Michel Hébert is a Research Director with the Information Security and Compliance practice at Info-Tech Research Group.

He helps IT leaders assess the maturity of their security environments, devise strategies to address shortfalls, and improve ransomware resilience.

Who is Info-Tech Research Group?

www.infotech.com

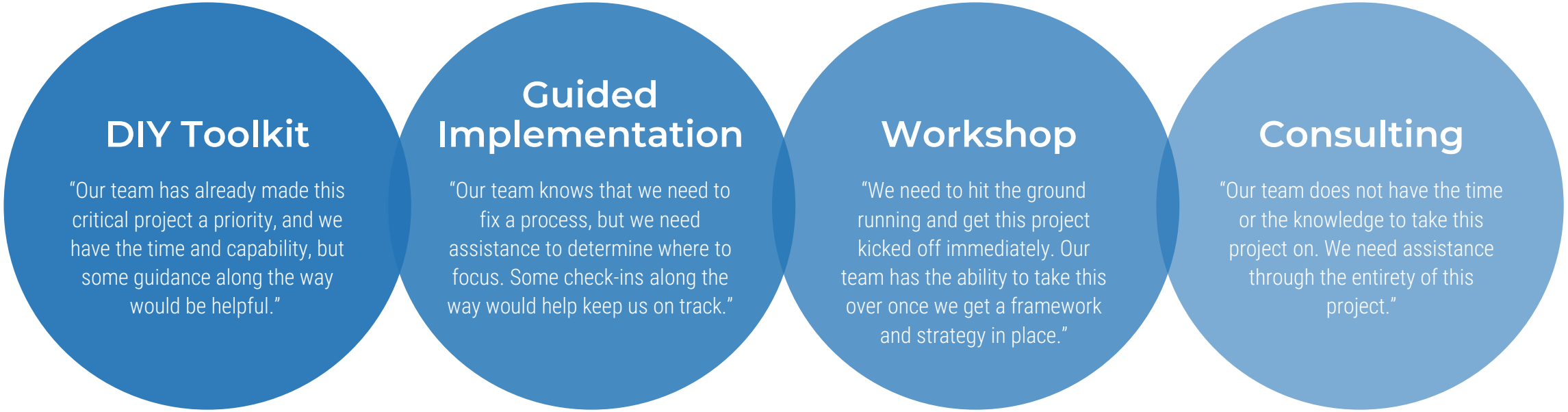
- Technology research and advisory firm.
- Opened our doors in 1997. Now more than 40,000 members worldwide.
- Help IT leaders improve their organizations systematically with practical guidance and balanced, high-quality research.

Getting to know each other

Introductions, please.

- Name
- Role
- Workshop thoughts:
  - Great if…
  - Worried that…

Info-Tech offers various levels of support to best suit your needs



I prepared a shared folder of resources for distribution after the workshop.

Reach out to mhebert@infotech.com if you would like to receive access.

Info-Tech's methodology for Creating a Ransomware Incident Response Plan

	Assess your ransomware readiness	Conduct a BIA to raise risk awareness and set recovery targets	Create a ransomware response workflow and runbook	Build a project roadmap to close gaps
Phase Steps	1. Conduct a maturity assessment 2. Review selected systems and dependencies	1. Record systems and dependencies in Info-Tech's *DRP Business Impact Analysis Tool* 2. Complete the impact analysis for selected systems and data sets	1. Document your threat escalation protocol 2. Use tabletop planning to identify response steps and gaps 3. Update your ransomware response workflow and runbook	1. Identify initiatives to improve ransomware readiness 2. Prioritize initiatives in a project roadmap 3. Communicate your current status and recommendations
Phase Outcomes	• Maturity assessment (includes identifying policy and technology gaps)	• Business impact analysis	• Tabletop planning results • *Ransomware Response Workflow* • *Ransomware Response Runbook*	• *Ransomware Project Roadmap* • *Ransomware Readiness Summary*

Note: This research can be executed as a do-it-yourself project, a Guided Implementation (series of advisory phone calls), or a facilitated Info-Tech Workshop.

Workshop Agenda

Ransomware Trends	• Introduce workshop and expected outcomes. • Review ransomware trends
Protect	• Review best practices • Conduct a high-level ransomware gap analysis • Identify potential impact of a ransomware attack.
Respond	• Review response workflow and runbooks
Test	• Conduct tabletop exercise to assess your current ransomware incident response plan for gaps.

The schedule will be flexible.

I planned for two 15-minute breaks and 45 – 60 minutes for lunch.

Ransomware

Primer and Trends

Pre-Mortem: Negative Visualization

Work through possible bad future scenarios so that you will be able to stay cool and respond in the best way possible when they occur.

Ransomware is all over the news

Why are so many organizations unprepared for an attack?

"Ransomware attack hits school district twice in 4 months"
(Associated Press, 10 Sept. 2019)

"Louisiana Suffers Another Major Ransomware Attack"
(Forbes, 20 Nov. 2019)

"British banks hit by hacking of foreign exchange firm Travelex"
(CNBC, 9 Jan. 2020)

"Florida city will pay hackers $600,000 to get its computer systems back"
(Washington Post, 20 June 2019)

"Ryuk Ransomware Uses Wake-on-Lan To Encrypt Offline Devices"
(Bleeping Computer, 14 Jan. 2020)

"Ransomware Gangs Now Outing Victim Businesses That Don't Pay Up"
(Krebs on Security, 16 Dec. 2019)

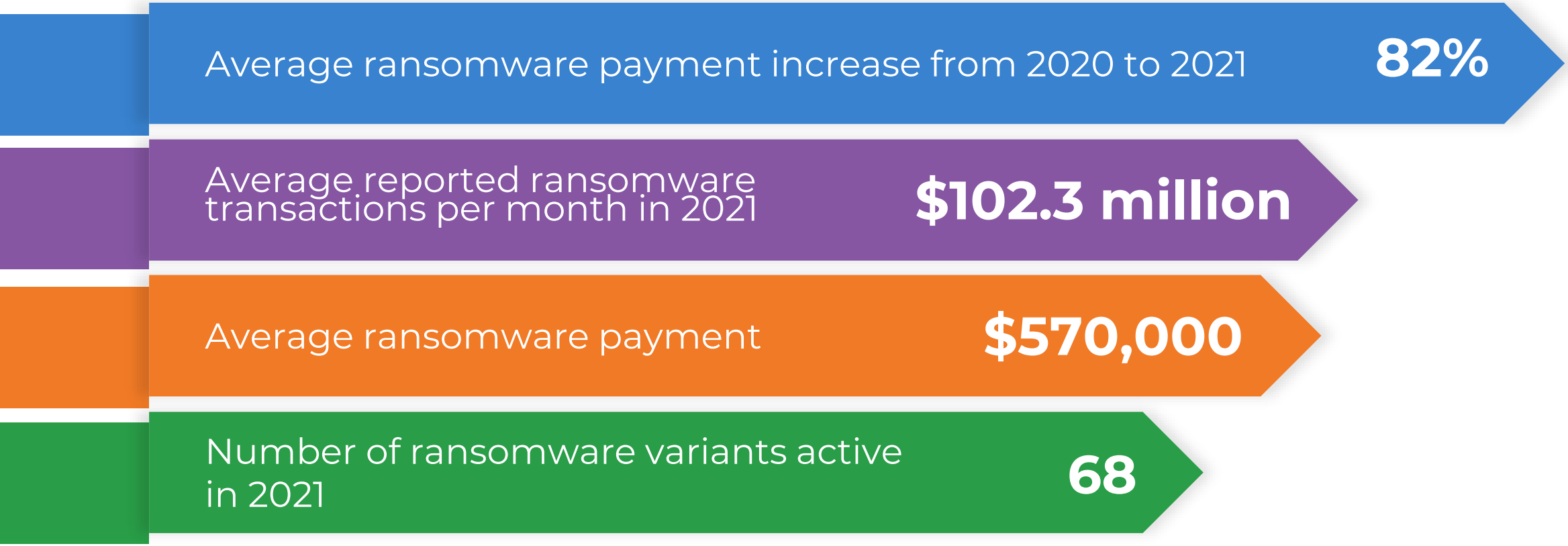
"Sodinokibi Ransomware Publishes Stolen Data for the First Time"
(Bleeping Computer, 11 Jan. 2020)

"Company shuts down because of ransomware, leaves 300 without jobs just before holidays"
(ZDNet, 3 Jan. 2020)

" 'Chaos is the Point': Russian Hackers and Trolls Grow Stealthier in 2020"
(The New York Times, 10 Jan. 2020)

The grim stats

The volume of ransomware attacks and their impact are increasing at alarming rates. Organizations are not ready.



Source: FinCEN, 2021, Palo Alto

Ransomware timeline – first half of 2021

Target: Kia Motors
Ransom: $20M demanded
Attacker: DoppelPaymer
Details: Large amounts of data stolen and encrypted. Disclosure/destruction of data threatened if payment not made.

Target: CNA
Ransom: $40M paid
Attacker: Evil Corp
Details: Attackers employed Phoenix CryptoLocker – a new ransomware variant – to encrypt over 15,000 devices including remote devices connected via VPN.

Target: JBS Foods
Ransom: $11M paid
Attacker: REvil
Details: JBS Foods, the largest beef supplier in the world, had operations suspended for several days following the attack.
Reportedly JBS was able to recover but paid the ransom to ensure no data was exfiltrated.

Target: AXA
Ransom: Unknown
Attacker: Avaddon
Details: This attack on the giant insurance provider AXA aligned with announcement of its new policy to exclude ransomware reimbursement from cyberinsurance coverage.

Target: Kaseya
Ransom: $70M demanded
Attacker: REvil
Details: Kaseya, an IT management platform, reported infections via its VSA data management and remote monitoring software across an estimated 1,000 businesses worldwide.

February | March | April | May | June

Target: CD Projekt Red (CDPR)
Ransom: No intention to pay
Attacker: HelloKitty gang
Details: Hacker group accessed intellectual property and threatened to release CDPR's product source code and embarrassing internal documents.

Target: Colonial Pipeline
Ransom: $4.4M paid
Attacker: DarkSide
Details: This was one of the most impactful ransomware attacks to date, as Colonial Pipeline's critical infrastructure role had widespread effects on the American public.

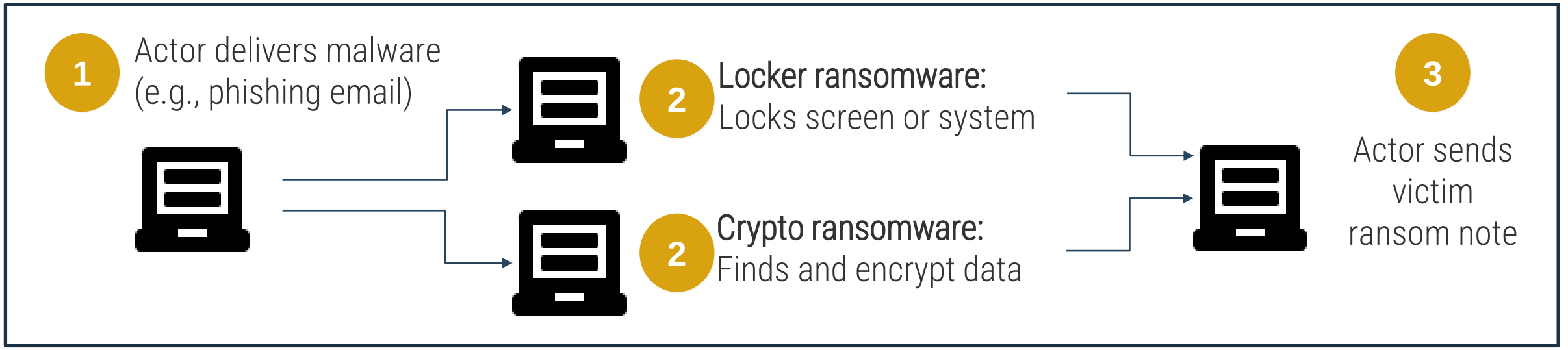
Target: Brenntag
Ransom: $4.4M paid
Attacker: DarkSide
Details: The same group who attacked Colonial received a large payment from Brenntag just the next month.

Target: Waikato District Health Board
Ransom: Unknown
Attacker: Suspected Conti Ransomware (Russia-based Wizard Spider cybercrime gang)
Details: Conti malware is a ransomware that looks to both steal information and encrypt your files and systems, with the threat of both denying you access to your own data and potentially publishing it or selling it.

Reference: Defend against the evolving threat of ransomware.

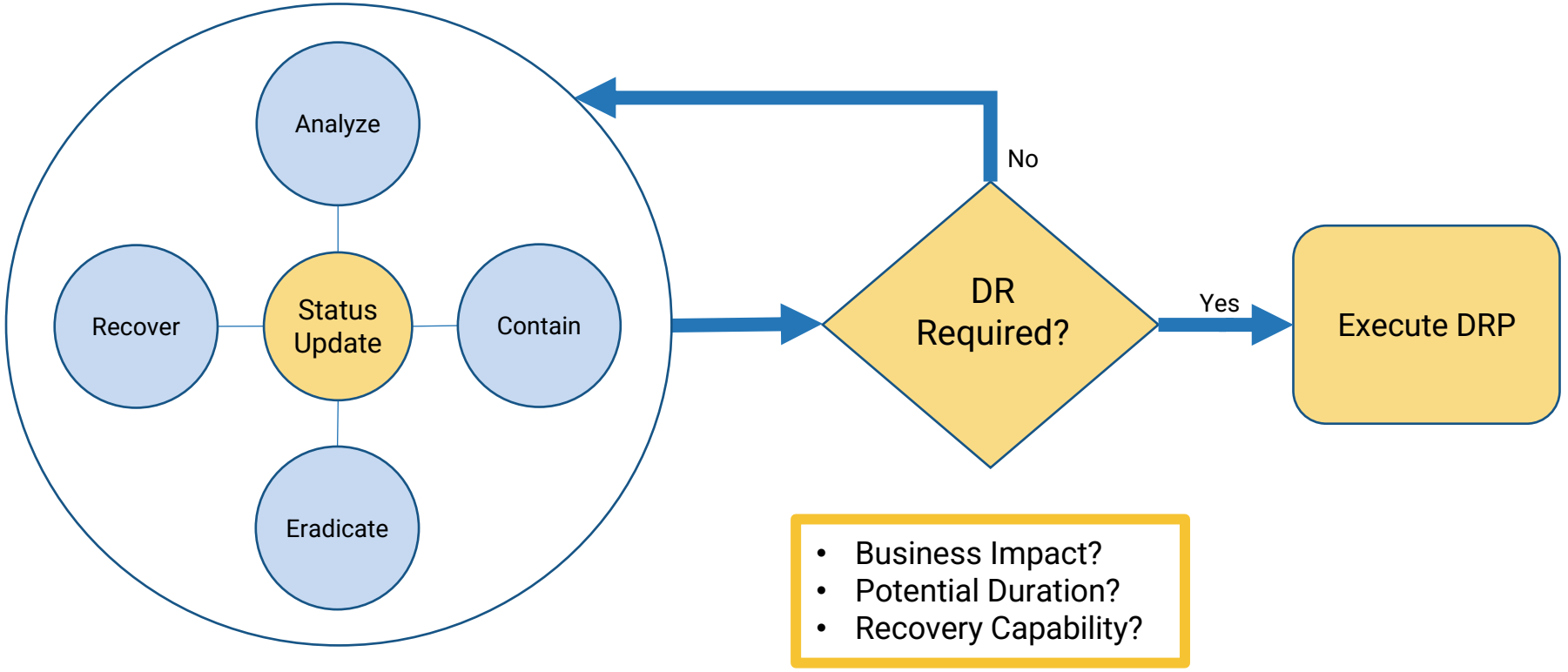
Level-setting

High-level illustration of a basic ransomware attack.



- **Ransomware:** Malware that locks systems or encrypts data for extortion or espionage.
- **Typical attack vectors:** remote desktop protocol, email phishing, software vulnerabilities, drive-by downloads, USB and removable media.

Resilience depends on protection, response and recovery



Anatomy of a ransomware attack

INITIAL ACCESS

EXECUTION

Deliver phishing email designed to avoid spam filter

Launch malware undetected with legitimate commands

PRIVILEGE ESCALATION

Run a net user command to identify user accounts

Find a target admin account (e.g., a default admin account for a recently added service)

CREDENTIAL ACCESS

Use brute force tactics (e.g., password guessing, cracking, and spraying, or credential stuffing) to crack the account

LATERAL MOVEMENT

COLLECTION

rights to move through the environment and collect data

Infect as many critical systems and backups as possible to limit recovery

DATA EXFILTRATION

DATA ENCRYPTED FOR IMPACT

Exfiltrate data undetected to gain leverage

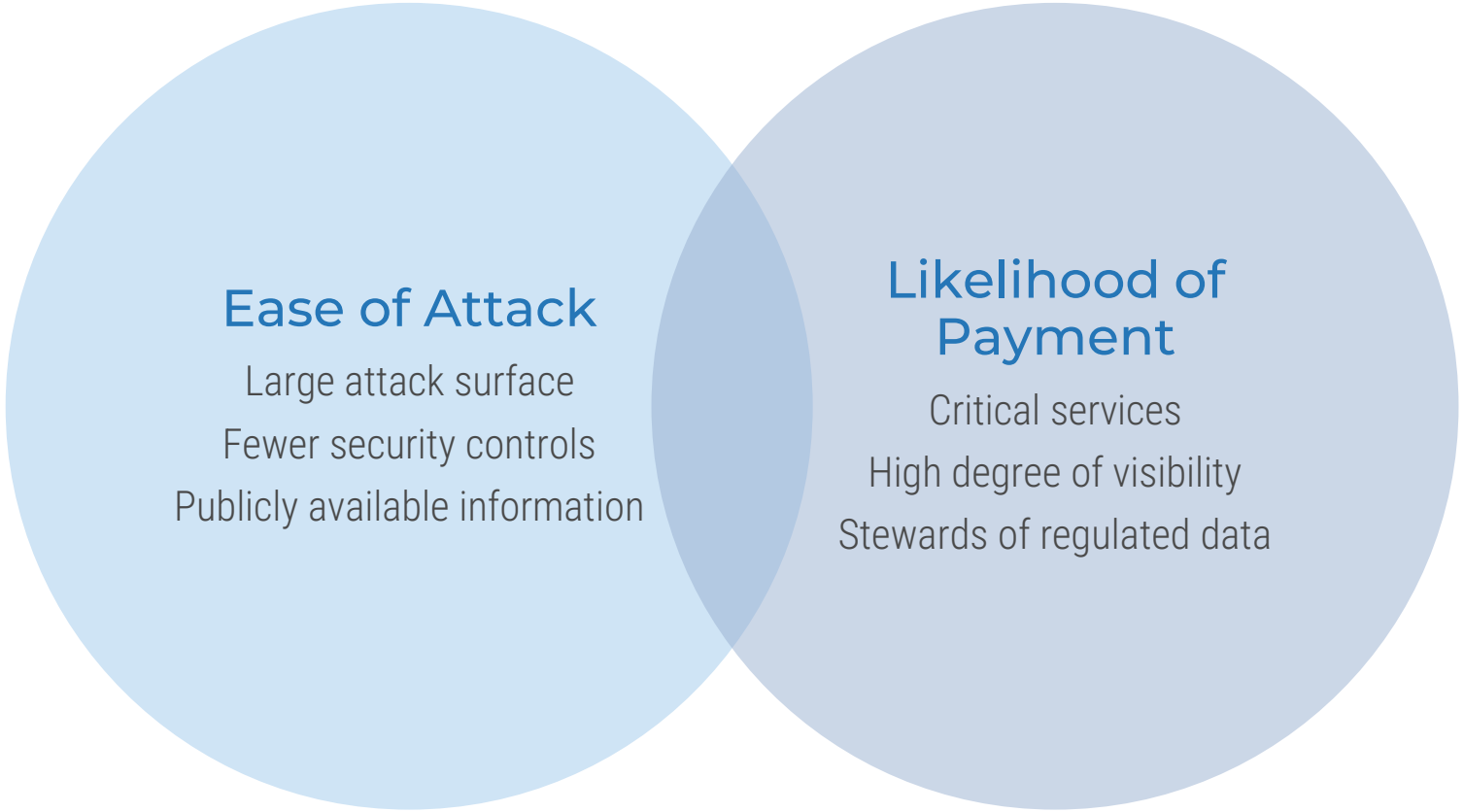
Encrypt data, which triggers an alert

Deliver ransom note

Reference: Threat Preparedness Using MITRE ATT&CK®, Defend Against the Evolving Threat of Ransomware

Trends and attack vectors

Gangs are using traditional attack vectors, but target profiles are changing



Supply chain, critical infrastructure, and organizations with regulated data are increasingly attractive targets.

Latest high-profile attacks also targeted MSPs and IT asset monitoring platforms.

Vendors often harden the security of their products and services but leave their own operations vulnerable.

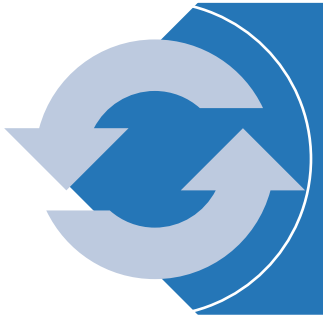
Case Study: Colonial Pipeline

	1. Compromise	2. Detection	3. Response & Recovery
Situation	1. FireEye confirmed that a compromised password led to the initial breach. The credentials were linked to a disused VPN account that lacked MFA protection. 2. No indications of phishing are reported; however, the password was published to the dark web as part of a set of leaked passwords.	1. In the early hours of Friday, May 7, the ransom demand was detected by a control room employee via a pop-up message on a control room device. 2. Within an hour, Colonial Pipeline had shut down its systems to contain the event.	1. One day after detecting and containing the malware, Colonial paid the ransom of $4.4M. 2. It is not clear whether Colonial chose to pay because it was unable to restore systems from backups, whether the recovery time would have excessively impactful, or whether the exfiltrated data prompted payment.
Challenges	DarkSide are a "Ransomware as a Service" gang, whose tactics are generally ransomware and digital extortion. The first step in their typical attack chain is typically one of three methods: 1. Brute force or leaked password attack 2. Phishing attack with malicious links 3. SQL-injection attacks against VPN infrastructure	Most of DarkSide's malware code is encrypted itself, which allows it to evade detection by endpoint protection – this and other anti-detection techniques are common amongst modern ransomware.	Critical infrastructure, supply chain, and large enterprises incur huge losses from downtime and face pressure to restore availability – attackers know this. Colonial faced enormous pressure to restore services, and it's possible that recovery capabilities were insufficient to meet the requirements.
Lessons	**Phishing** and **identity-based attacks** are still the main point of entry for ransomware attackers.	Ransomware is evolving to evade detection and complicate system restoration.	The difference between organizations who pay a ransom and those who do not often comes down to whether they are **prepared** and able **to respond and recover.**

The challenge with ransomware

Multiple attack vectors. Ransomware dormant, infiltrating backups, DR sites, and more endpoints before activation.

Data loss is bad; data loss plus the inability to restore from backups is devastating. Your systems could be down until “clean” data restoration is made from an historic recovery point.



Ransomware is constantly evolving but best security and continual improvement practices are still effective.

Ransomware

Reduce your exposure

Compromise:

Focus on **strong identity controls** and **end-user security awareness training**

Detection:

Focus on **endpoint detection and response** capabilities

Recovery:

Build a **DRP**, update the **backup strategy**, invest in **immutable back-ups**

Reduce your exposure

Make yourself less of a target. Threat agents may look for an easier target.

- **Traditional perimeter and endpoint security still matter.** They block attacks every single day.
- **Follow standard security best practices.** Design, deploy and enforce security policies to mitigate security risks. Segment your network, implement a least-privilege access policy to limit admin rights, and put in place a security awareness training program for end users.
- **Supplement the basics with advanced threat detection tools.** AI-based security monitoring is the countermeasure to attacks designed to bypass traditional endpoint security.

Business-Aligned.

Determine business context and cascade enterprise goals into security alignment goals.

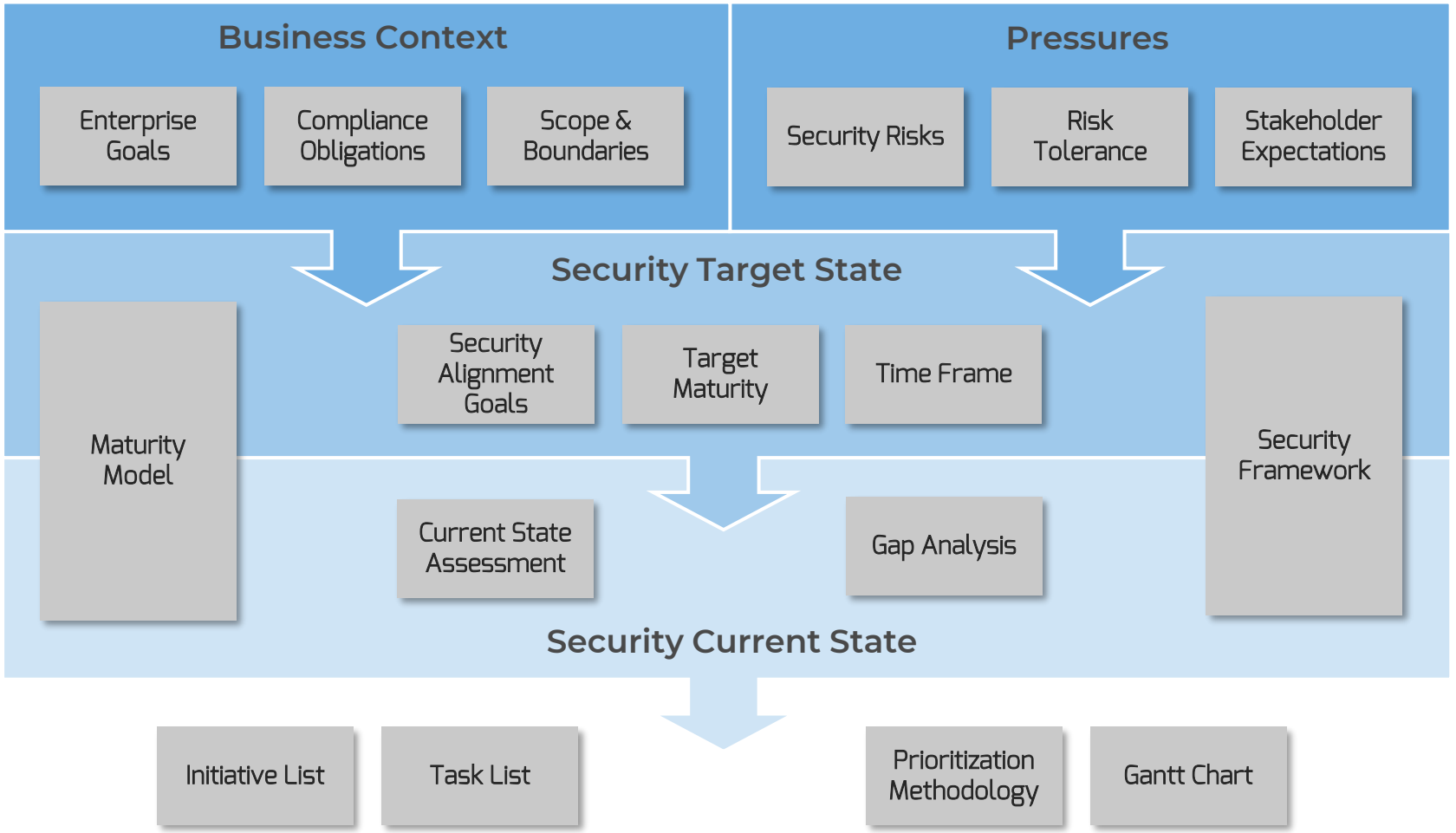
Risk-Aware.

Understand the security risks of the business and how they intersect with the overall organizational risk tolerance.

Holistic.

Use a best-of-breed information security framework to provide comprehensive awareness of organizational security capabilities.

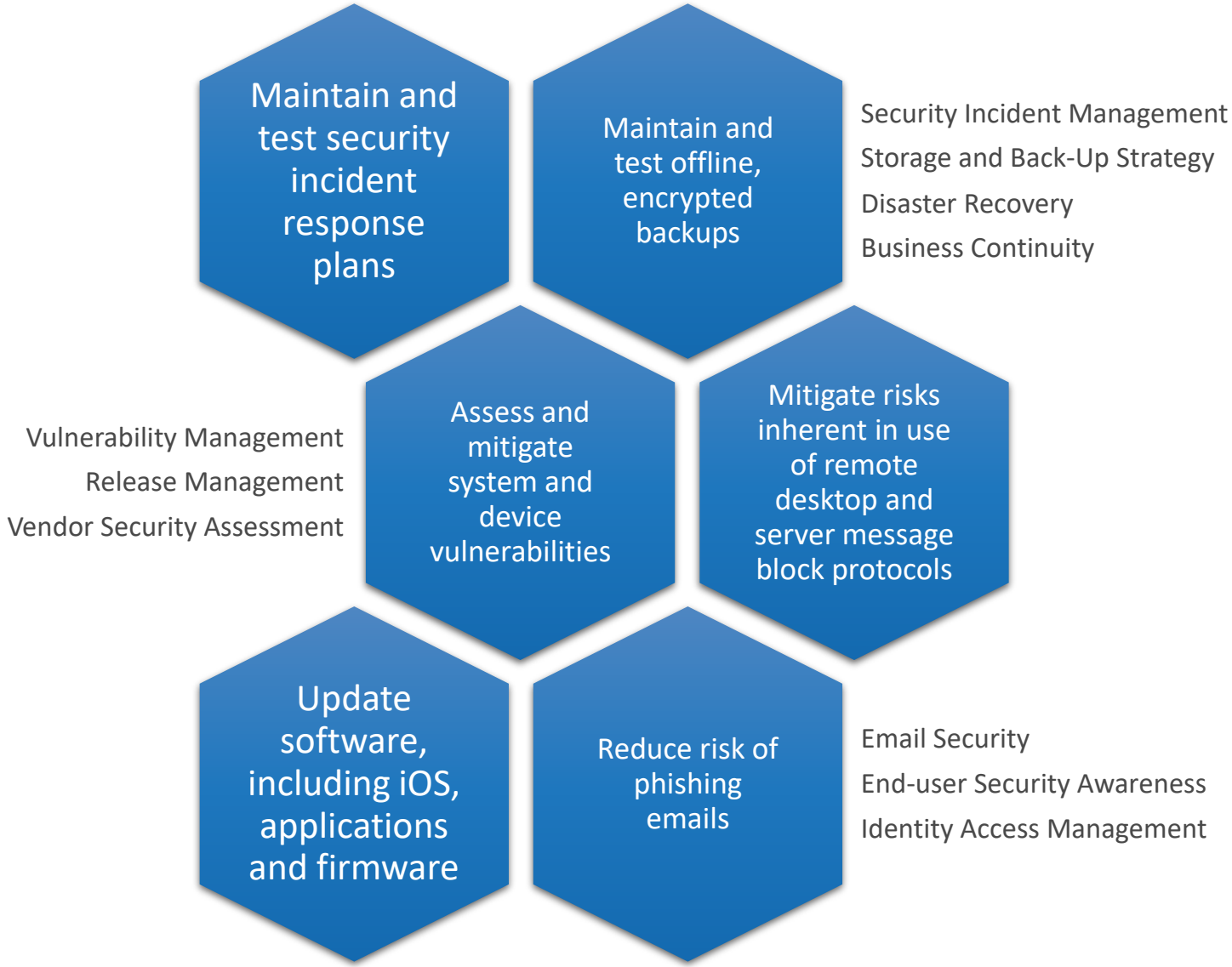
Align your strategy to organizational goals to communicate your vision



Reduce your exposure

Sources:

- The NIST preliminary draft cybersecurity framework profile for ransomware risk management
- CISA security fact sheet on preventing data exfiltration.



Why are so many organizations unprepared for ransomware attacks?

Despite the attention on Ransomware, many are falling victim to known vulnerabilities

City of Atlanta, 2018:

Two months before the city of Atlanta was hit by ransomware in 2018, an **audit identified over 1,500 severe security vulnerabilities**.

City of Baltimore, 2019:

Before the city of Baltimore suffered multiple weeks of downtime due to a ransomware attack in 2019, a **risk assessment identified a severe vulnerability due to servers running an outdated operating system** (and therefore lacking the latest security patches) and **insufficient backups to restore those servers if necessary**.

Failing to present risk in business terms to get appropriate security funding and policies.	Conduct a BIA to highlight business risk – financial impact and reputational damage
Not going deep enough in testing ransomware readiness	In addition to pen testing, conduct regular tabletop planning exercises to validate and improve your incident response plan
Backup strategies and DR plans don't account for ransomware scenarios	For your critical data, ensure multiple restore points that includes an immutable backup

Three common mistakes in ransomware security planning

Improve Ransomware Resilience

Build Layered Defenses

THREAT PREPAREDNESS

Review ransomware threat techniques and prioritize detective and mitigation measures for initial and credential access, privilege escalation, and data exfiltration.

AWARENESS & TRAINING

Develop security awareness content and provide cybersecurity and resilience training to employees, contractors and third parties.

PERIMETER SECURITY

Identify and implement network security solutions including analytics, network & email traffic monitoring, and intrusion detection & prevention.

OPERATIONAL RESILIENCE

Identify disruption scenarios and develop incident response, business continuity, and disaster recovery strategies.

ACCESS MANAGEMENT

Review the user access management program, policies and procedures to ensure they are ransomware-ready.

VULNERABILITY MANAGEMENT

Develop proactive vulnerability and patch management programs that mitigate ransomware techniques and tactics.

Ransomware

Tabletop Planning

Tabletop Exercise

Format:

1. Three SLT “briefings”
    A. Initial escalation
    B. Two subsequent updates based on expanded knowledge
2. Each briefing contains
    A. Current known scope/impact
    B. Potential exposures and anticipated next steps
    C. Decision/Discussion points

Goals:

1. Familiarize this team with the “flow” of an incident and forensics
2. Identify gaps/uncertainties to close now
3. Make decisions for organization based on risk
4. Prepare for communications – with each other, employees, members, etc.
5. Set collaboration expectations and SLAs – with MSP/MSSP/forensics
6. Identify where your response plans/contact info are located
7. Share details of assistance options – forensics, insurance, legal, etc.

Tabletop Exercise

Initial Update

Monday, 11:00am

1. End user report in morning of failed access to N:drive received by Product Success/Help Desk – 8:30AM
2. Reports from other end users came in and Product Success/Help Desk escalated to Directors of Technology/InfoSec Operations – 9:00AM
3. InfoSec Operations investigated further. Indications there is malware spreading across systems and encrypting files. Reached out to MSSP for analytic assistance.
4. Technology team has isolated systems in N:drive to minimize further spread.
5. Service advisory to employees about systems down while we work on it, with regular updates.
6. We suspect ransomware, although no demand has been revealed yet.

Discussion Points:

1. What message should we provide to employees?
2. Do we expect membership visibility of any issue?
3. What regulatory or contractual impacts should we consider? (HIPAA, GDPR, PCI, Member Data, Trade secrets…)
4. Who contacts cyber insurance and when? What can we expect from them?
5. Should we engage forensics firm yet for assistance?

Tabletop Exercise

Second Update

Monday, 5:00pm

1. Looking at other systems where initial infected account has access – O365, membership system, finance system, etc.
2. We've engaged with insurance and MSP/MSSP and forensics firm, and we have consultants assisting with analysis
3. Timeframe to determine extent and starting time for the introduction of the malware/ransomware program is still TBD
4. Considerations:
   A. Friday 10AM is our initial guess for clean point for data restoration – losing updates since then
   B. Will need to rebuild servers and restore data – will take time and systems continue to be unavailable during this effort

Discussion Points:

1. What message should we provide to employees at this time?
2. What message might we prepare for members?
3. What regulatory or contractual impacts should we consider?
4. Which are our most critical systems/data to recover?
5. What do the restoration timelines look like?
6. If PII/confidential data was involved/stolen, what are considerations?

Tabletop Exercise

Third Update

Tuesday, 10:00am

1. We've received ransom demand of 1Bitcoin for decryption key
2. No claim yet of stolen data and forensics team investigation includes looking for evidence of data exfiltration.
3. Forensics team is providing direction about infection time and systems

Discussion Points:

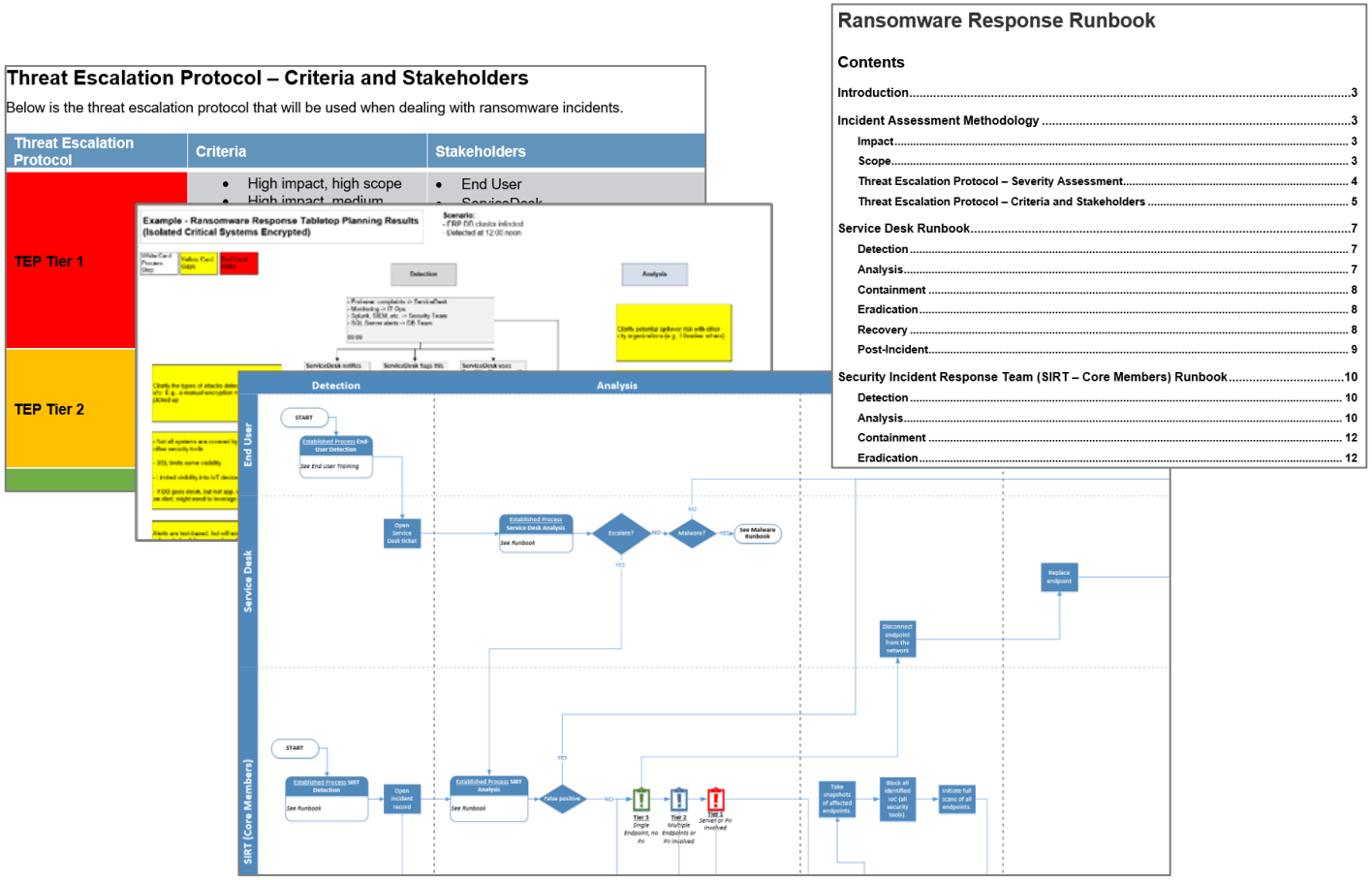
1. Are we notifying law enforcement/FBI of ransom demand? (Who?)
2. What aspects are part of consideration for any ransom payment decision?
3. Will BC/DR teams be available to test functionality of recovered systems?
4. Will BC processes identify how to restore lost work after systems were shut down and since then (if still manual)
5. How are we tracking expenses for the insurance claim?

Ransomware

Workflows and Runbooks

Practice makes permanent

- Review threat escalation protocols
- Walk through response steps to a potential ransomware incident
- Identify gaps in runbooks and workflows
- Update plans
- Record residual risks



Threat Escalation Protocol – Criteria and Stakeholders

Below is the threat escalation protocol that will be used when dealing with ransomware incidents.

Threat Escalation Protocol	Criteria	Stakeholders
TEP Tier 1	• High impact, high scope	• End User
TEP Tier 2		

Ransomware Response Runbook

Contents

INFO~TECH
RESEARCH GROUP

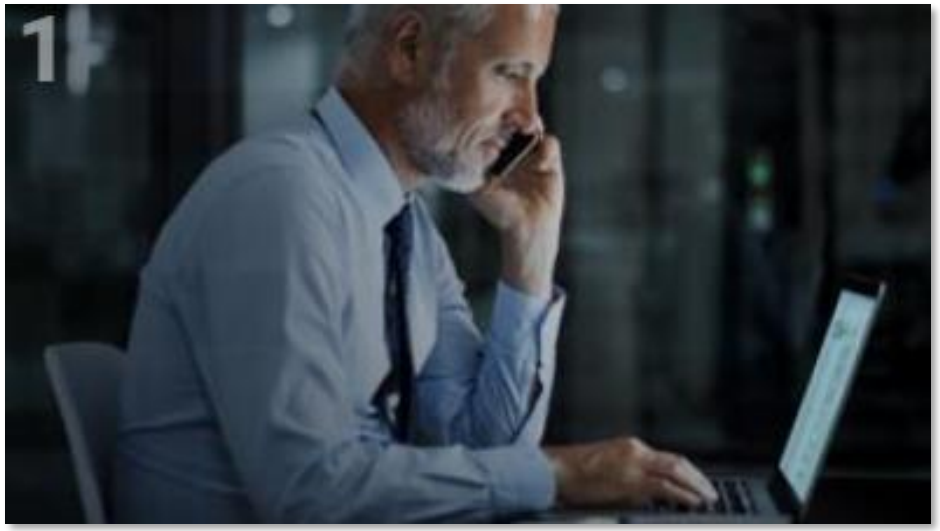
Michel Hébert, PhD

Research Director, Security, Privacy, Risk and Compliance

Email: mhebert@infotech.com

LinkedIn: smichelhebert/

Related Info-Tech Material



[Create a Ransomware Incident Response Plan]

[Threat Preparedness Using MITRE ATT&CK®]

[Defend Against the Evolving Threat of Ransomware]

[Develop and Implement a Security Incident Management Program]

[Build a Vendor Security Assessment Service]

[Create a Right-Sized Disaster Recovery Plan]