bpm

# Managing cyber-risk?

*There’s no such thing as done.*

Cybersecurity Update

December 2023

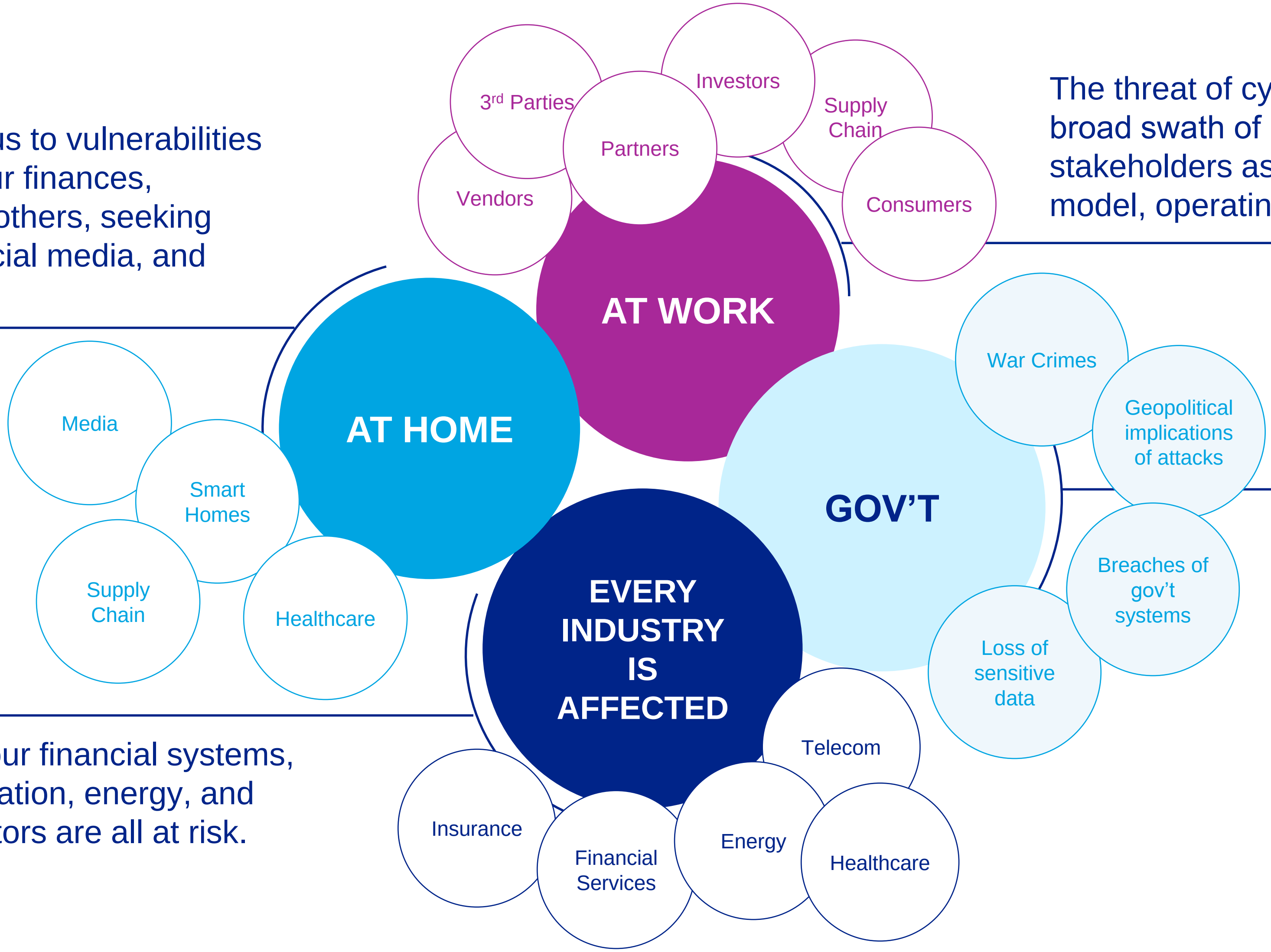
# I’m not telling you its going to be easy, I’m telling you its going to be worth it….

> “Why do you rob banks?”
>
> *“Because that’s were the money is.” Willie Sutton*

# In today's world, everything is connected, systems are complex, and cybersecurity touches our lives on a massive scale…

Our actions expose us to vulnerabilities daily — managing our finances, communicating with others, seeking healthcare, using social media, and shopping.

The threat of cyber attacks impacts a broad swath of an organization's stakeholders as well as its business model, operating model, and strategy.



AT WORK

3rd Parties

Investors

Supply Chain

Partners

Vendors

Consumers

AT HOME

Media

Smart Homes

Supply Chain

Healthcare

GOV'T

War Crimes

Geopolitical implications of attacks

Breaches of gov't systems

Loss of sensitive data

EVERY INDUSTRY IS AFFECTED

Telecom

Insurance

Financial Services

Energy

Healthcare

Cybersecurity is of particular concern to our government as the impacts of cyber risk scale. Critical infrastructure and sensitive data are at risk.

No industry is safe: our financial systems, healthcare, transportation, energy, and communications sectors are all at risk.

# New “Threat Vectors” are accelerating concerns.

## YESTERDAY

**Bad “Actors”**

- Isolated criminals
- “Script Kiddies”

**“Target of Opportunity”**

**Targets**

- Identity Theft
- Self-Promotion Opportunities
- Theft of Services

## TODAY

**Bad “Actors”**

- Organized criminals
- Foreign States
- Hacktivists

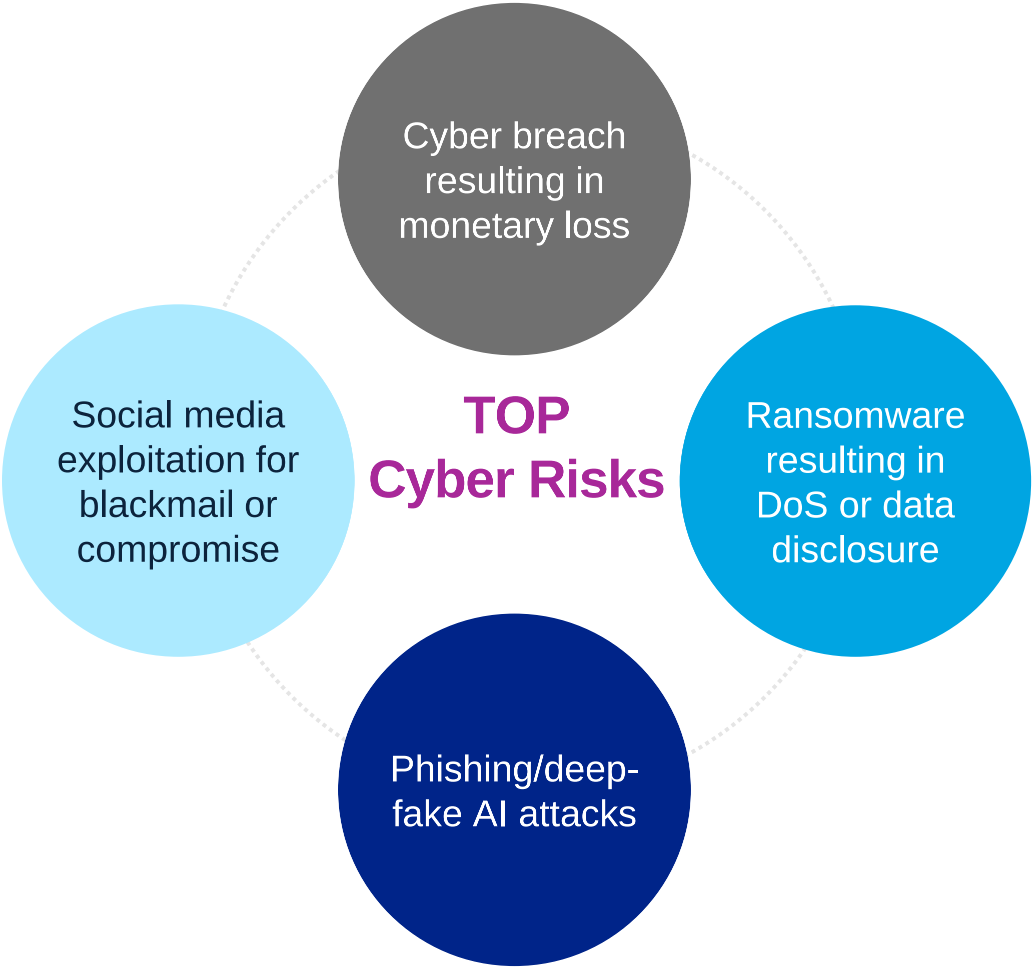
**“Target of Choice”**

**Targets**

- Extortion/Blackmail
- Financial Theft/Fraud
- Denial of Service

# What does this mean for your business?

- Cyber breaches resulting in financial loss due to wire fraud, unauthorized transfers or unauthorized disposition of assets
- Ransomware resulting in DoS, financial loss or data disclosures
- “Denial of Service” attacks on physical assets such as smart homes, yachts, vehicles, planes etc.
- Business email compromise leading to identity theft or financial loss
- Fraud perpetuated by trusted “insiders”
- Kidnapping and ransom due to unauthorized disclosure of travel plans, manifests, and/or social media posts
- Exploitation of social media accounts to stalk executives and/or steal compromising pictures or information



TOP Cyber Risks

Cyber breach resulting in monetary loss

Ransomware resulting in DoS or data disclosure

Phishing/deep-fake AI attacks

Social media exploitation for blackmail or compromise

# The Three Questions…..

Start thinking about cyber-risk by asking a few simple, but provocative questions …

**What are we doing?**

**Is it enough?**

**How do we know?**

If you can’t answer these questions definitively, it’s time for a closer look.

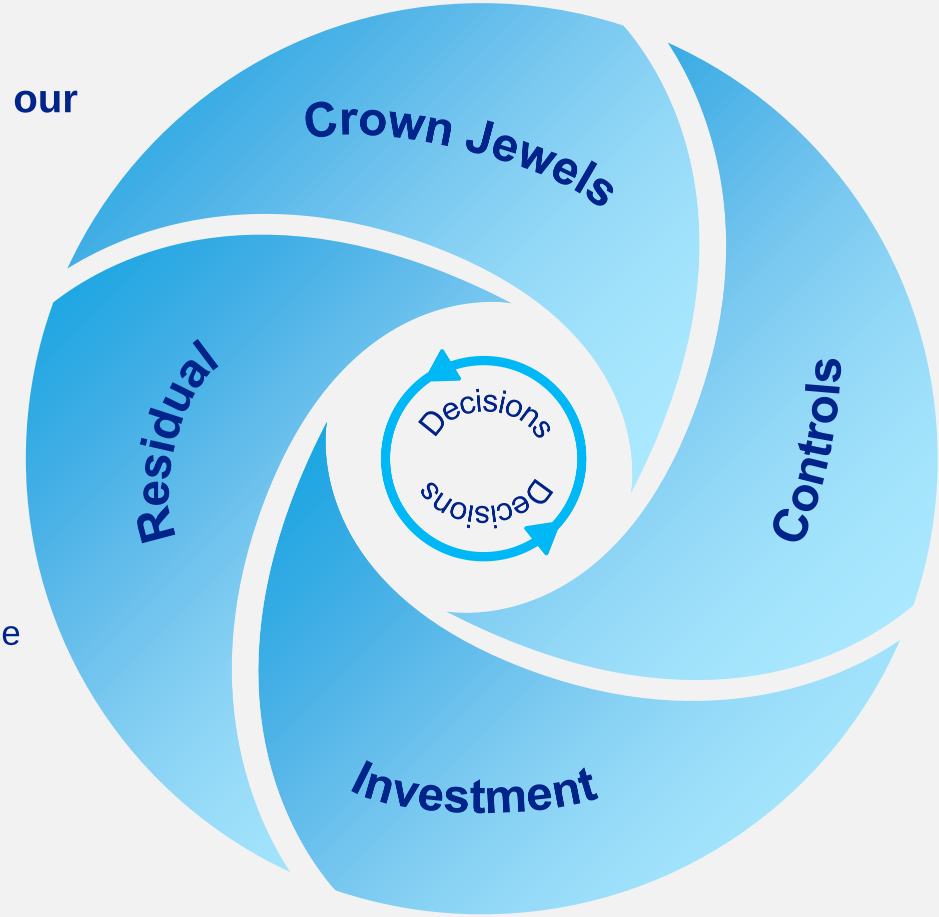
# Start with a risk assessment.

**Do we understand/have we identified our most valuable assets – our “crown jewels”?**

- Customer data
- Intellectual property
- Trade secrets

**What security and controls have we put in place and are they commensurate with the value?**

- Safe words/code words/challenge response
- Dual-factor authentication
- Encryption
- Access control
- What’s the routine?



**How much are we willing to spend?**

- Dedicated team
- Advanced technology
- Drills and rehearsals

**How much risk are we willing to “leave on the table”?**

- Risk tolerance
- Re-evaluate frequently

# A simple risk assessment framework

## What are we doing?

**1**

### Crown Jewel Assets

Have we identified the most valuable assets in the business? Do we know what is most critical? What would be most valuable to an adversary,

**2**

### Security and Controls

What controls have we put in place over those assets? Do we follow the rule of "least privilege"? Do we limit access to "need to know" only?

## Is it enough?

**3**

### Security investment

Have we assessed how much we currently invest in cyber? How much more or less are we willing to spend?

**4**

### Residual Risk

We cannot eliminate all risk. How much residual risk do we have? Are we comfortable, given our risk tolerance and the threats we face?

## How do we know?

**5**

### Practice and Test

Do we have outsiders assess our program and controls? Do we run rehearsals and other drills such as tabletop exercises? Who's on speed-dial if something goes wrong?

# Three keys to become more resilient

Mitigate the human variable though awareness and training

Invest in people and technology for better prediction, detection, and response

Develop a mindset of resilience: Assume if you haven’t been hit, you’re about to be.

# The Human Variable – Building Human Firewalls

T-Shirts and coffee mugs don’t cut it anymore

# Human variable

The human variable is a hard-to-control input into cybersecurity, as humans are inherently unpredictable and difficult to control.

People will click on anything for a free iPad.

Best ROI in cybersecurity? It's still from training and awareness.

## Moving past the "human factor is the weakest link" trope to business enablement and "safe at home"

Attacks that exploit human propensity to make misjudgements remain prominent and effective — when all it takes is **one click to cause a breach**.

**38%** of U.S. cyber attacks involved **phishing scams** in 2021.

**98%** of breaches relied on some form of **social engineering** to be successful.

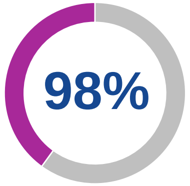
Employees are particularly vulnerable at home, creating security concerns as more people move out of the office to **work from home**.

**$1.07M** increase in the **cost** of a **data breach** if **remote work** was a factor in causing the breach.

People are adopting a growing number of **devices,** increasing the number of pathways into their lives and data.

**55.7** *billion* **connected** devices by 2025, 75% of which will be IoT devices.

This grows every individual's cybersecurity responsibility, highlighting the importance of a educated and aware user.



of **IoT traffic** is **unencrypted,** which accounts for **72 zettabytes** of transmitted unencrypted **data** by 2035

Sources: Purplesec, Tessian, Security Intelligence, IBM, IDC, Palo Alto Networks

# Conscious choice to a habit

**Key success factors of leading programs. (Hint: It’s a process, not an event.)**

- Support from principals and senior leaders
- Everybody is involved
- Behavior matters — but technology helps
- Be consistent and persistent
- Culture - It’s how we do business
- Make it personal
- Positive reinforcement

# “We don’t have brakes so we can go slow. We have brakes so we can go fast.”

## Business enablement

- Focus not on what we can’t do, but on **what we *can***.
- Cybersecurity is not about “No.” It’s about about “Yes, and …”
- Cybersecurity is a way to be “better, faster, stronger,” allowing the organization to do more.

## Safe at home

- CISO of your home: ***You*** are the Chief Information Security Office!
- Remote work has created new cyber challenges for employees.
- ***Make it personal!*** Engagement around cyber-risk management increases when employees feel like the organization is looking out for them.
- “**Safe at home**” training, focused on identifying and avoiding scams and other malicious activity

***“Make it known. Make it clear. Make it real. Make it stick. Make it happen.”***

# Should I Pay the Ransom?

Maybe – but probably

# You’re Going to Get Popped.

## Hope is *not* a strategy …

> “Everyone has a plan until they get punched in the face.”
>
> *— Mike Tyson*

> “In preparing for battle I have found that plans are useless, but planning is indispensable.”
>
> *— Dwight D. Eisenhower*

# Ransomware trends

## Most common 2022 root causes:

1. Phishing
2. Unpatched vulnerability exploitation
3. Systems misconfiguration/poor password management

## Ransomware

disproportionately affects small and medium sized businesses.

## Most targeted:

1. Professional/legal services firms
2. Finance
3. Healthcare

Firms, on average, have experienced **20 days** of downtime.

Almost **50%** of ransomware cases included the threat to release exfiltrated data, i.e., **layered extortion model.**

**80% of organizations** end up wanting to pay the ransom and don’t even know how.

**Threat actors collaborate to provide “professional services” to each other.**

***During a ransomware attack, different threat actors may operate in your environment — e.g., a group that writes malicious tools (weaponization), one that penetrates your network (access brokers), and one that distributes the ransomware. Technically, these are separate entities selling competencies to each other.***

# Not if, but when….

**CNN reported that "Ransomware gangs like to strike on the weekend or during holidays, when organizations are short-staffed and potentially off-guard."**

**Invasive**

- Ransomware offered as a service
- Makes capability readily available

**Pervasive**

- Attackers spend more time in systems
- Increasingly stealing data for blackmail
- Targeting key systems and backups

**Inevitable**

- Ransom demands growing
- Linked to threats of data disclosure
- Greater business disruption

Average cost of a data breach in the US: **$9.05M**

Average dwell time: **78** days

Average time to respond to a cyber incident: **212** days

Average time to recovery: **287** days

**Most common 2022 root causes:**

1. Phishing
2. Unpatched vulnerability exploitation
3. Systems misconfiguration or poor password management

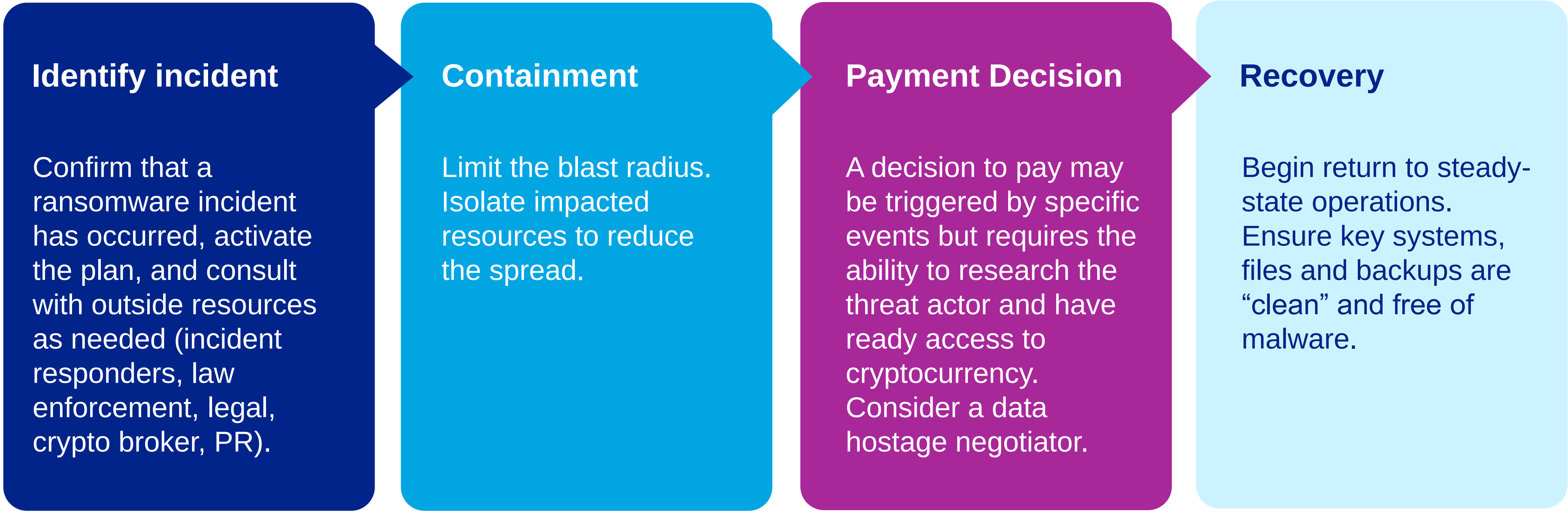
*Source: IBM Security – Cost of Data Breach 2021*

# Ransomware Response

**DailyDot reported - Ransomware gang files complaint with SEC complaining victim didn't promptly announce breach. The cybercrime gang claims its victim 'has not fulfilled' their obligation to report the breach.**

## Roles and Responsibilities

Having a plan, with clearly defined roles and responsibilities, can significantly reduce the impact and duration of a cyber event. **And practice, practice, practice …**



### Identify incident

Confirm that a ransomware incident has occurred, activate the plan, and consult with outside resources as needed (incident responders, law enforcement, legal, crypto broker, PR).

### Containment

Limit the blast radius. Isolate impacted resources to reduce the spread.

### Payment Decision

A decision to pay may be triggered by specific events but requires the ability to research the threat actor and have ready access to cryptocurrency. Consider a data hostage negotiator.

### Recovery

Begin return to steady-state operations. Ensure key systems, files and backups are "clean" and free of malware.

# AI – The brave new world

Deep fakes and other threats

# Deep Fake Hacking

**Cybersecurity Risks**
Deep fakes can be used in cyberattacks in which attackers impersonate company executives or employees to gain access to sensitive information or initiate fraudulent transactions.

**Identity Theft**
Deep fakes can be used to create realistic forgeries of identification documents, making it easier for criminals to engage in identity theft or fraud.

**Ransom Attacks**
Criminals can threaten to release damaging deep fake content unless victims pay a ransom, adding a new dimension to extortion schemes.

**Social Engineering Attacks**
Cybercriminals can use deep fakes to impersonate trusted individuals, such as friends or family members, to manipulate targets into revealing personal or financial information..

**Misinformation / Fake News**
Deep fakes can be used to create convincing videos or audio recordings of public figures saying or doing things they never did. This can lead to the spread of false information, influence elections, and damage reputations.

**Reputation Damage**
Deep fakes can tarnish the reputations of individuals and organizations by falsely implicating them in inappropriate or illegal activities.

**US mother gets call from ‘kidnapped daughter’ – but it’s really an AI scam – *The Guardian***

Jennifer DeStefano tells US Senate about dangers of artificial technology after receiving phone call from scammers sounding exactly like her daughter.

# Simple but effective….

Establish "safe words" for communications including "under duress."

Challenge/response codes for financial or other sensitive transactions.

Establish a "process" for communications including "out of band."

## The broad spectrum of combating "deep fakes"….

### GOOD

Employee Awareness Training - teach employees to be skeptical

Access Control and Least Privilege - limit access to what is require for job function

Incident Response Plan - specific plan for deep fake attacks

### BETTER

Policies and Procedures – guidelines for identifying identities and sensitive transactions

Regular Software Updates – keep software up to date with patches and other upgrades

Email Filtering and anti-phishing/anti-spam software

### BEST

**Collaborate and consult – seek out experts in deep fake attacks to stay current on trends and defenses**

**Monitoring and Threat Intelligence – subscribe to a threat intel feed to be up to date on latest attacks or targeted attacks**

### OFF THE CHARTS

Email authentication – advanced email protocols (DMARC)

Multi-Factor Authentication – challenge/response tokens

Secure video conferencing – strong authentication and encryption

AI Based Detection Tools

# Wrap up….

If you remember nothing else…..

# Talking about Cyber…

Starting a conversation with a few simple, but provocative questions……

Are our people well trained, aware, alert and skeptical?

Can we respond to, and recover from, a ransomware attack?

## Things to consider…

- Quick start assessments and roadmap development.
- Deep dive assessments, exposure management and penetration testing, compliance management, threat assessment, ransomware, GRC and managed SOC.
- Knowledge and insight sharing sessions, executive education and outreach.

## Get started with the three questions:

1. *What are we doing?*
2. *Is it enough?*
3. *How do we  know?*

Remember – If you can't answer these definitively, it may be time for a closer look.

# Fred Rica

## Partner, Advisory

As a former big 4 Partner with over 30 years of experience I’ve had the opportunity to help clients address cyber and technology risk issues in identity management, vulnerability management, incident response, compliance management, organizational design and governance across a broad range of industries. I’ve been fortunate enough to help many of the world’s foremost users of technology, and some of the Fortune 500’s most recognizable brands, solve complex risk management issues in financial services, telecommunications, technology, consumer products, industrial manufacturing, government and multi-lateral organizations.

I have presented on the topic of cybersecurity at conferences like the Black Hat Briefings, been quoted in major print media and have appeared on CNN, CNBC, FOX and other major networks.

frica@bpmcpa.com

+19083103898

bpm

BECAUSE PEOPLE MATTER