The Changing World of Cyber Liability

cowbell®

Cowbell Contacts

Everett Finn

Territory Manager
everett@cowbellcyber.ai

Bimbola Afolabi

Sr. Cyber Marketing Manager
bimbola@cowbellcyber.ai

Imran Garrouch

Risk Engineer
imran@cowbellcyber.ai

Cyberattacks are painful problems….that are not going away

$2.2M

The annual costs of cybercrime to small and medium sized businesses [1]

95%

of cybersecurity breaches are caused by human error [2]

68%

of business leaders feel that their cybersecurity risks are increasing [3]

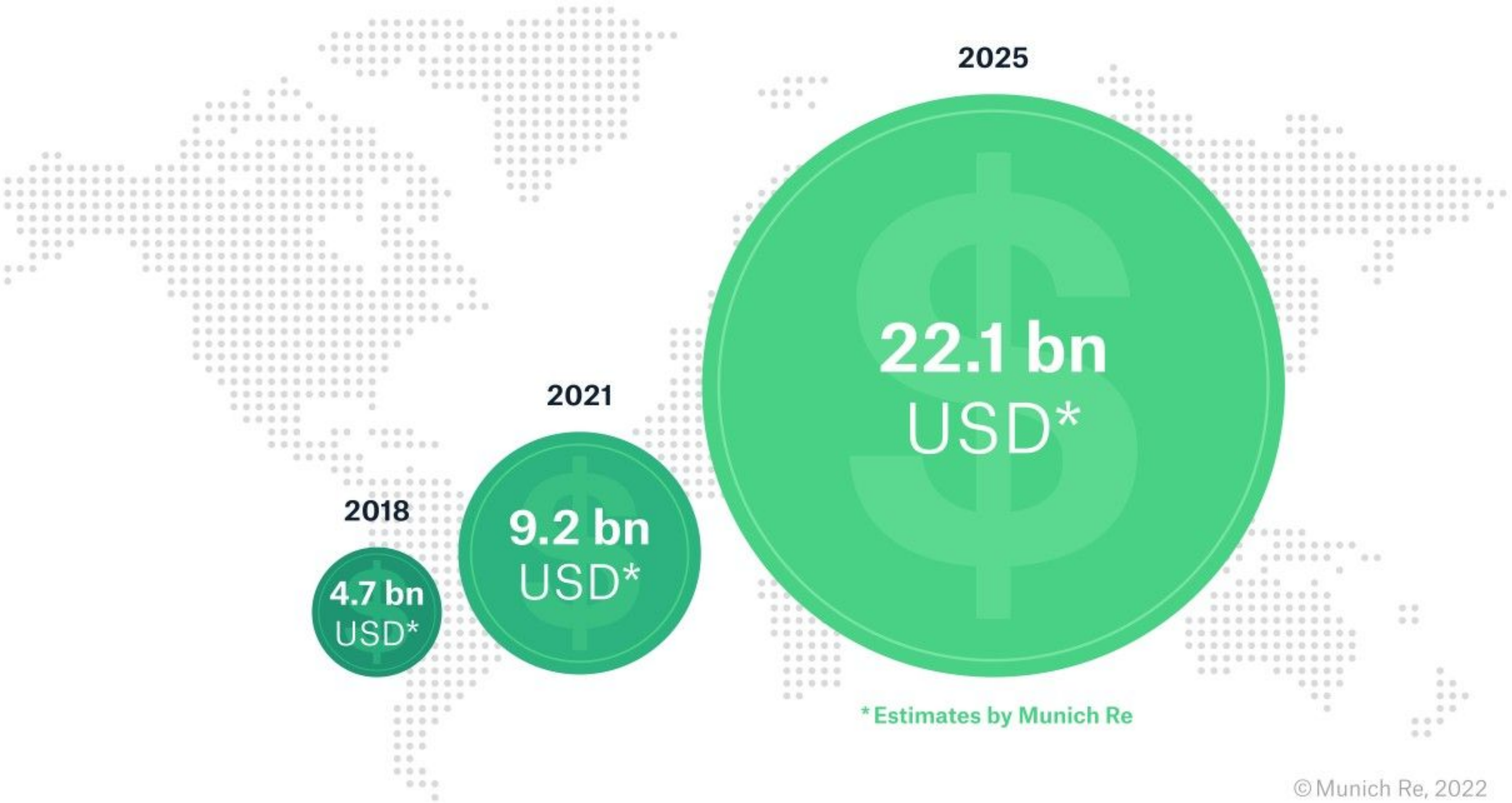
2,224

Hacking attacks occur every day – one every 19 seconds [4]

[1] https://www.fundera.com/resources/small-business-cyber-security-statistics
[2] https://www.cybintsolutions.com/cyber-security-facts-stats/
[3] 2. Accenture Security, The Cost of Cybercrime; https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
[4] University of Maryland; https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

Why is Cyber such a huge area of growth?

Global cyber insurance market with strong expected growth



* Estimates by Munich Re

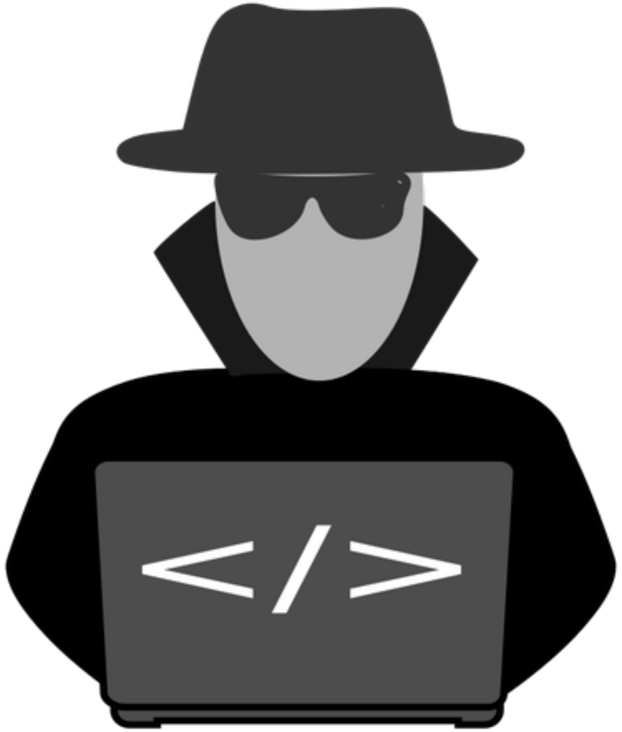
© Munich Re, 2022

Understanding Data Breaches

What do they want?

Valuable and sensitive data like:

- Personal Identifiable Information (PII)
  - Social Security Number
  - Passport Information
- Protected Health Information (PHI)
  - Medical Records
- Payment Card Information
- Employee Records
- Intellectual Property



Some common cyber risks..

Data Breaches

- ➔ Unauthorized access into systems can result in compromised client files, loss of sensitive data and could result in potential lawsuits from clients and seriously damage the firm's reputation.

Lost or Stolen Phone or Laptop

- ➔ With employees access to substantial client information, a stolen/lost device can compromise client information.

Ransomware

- ➔ Even after a ransom is paid, important data/ sensitive information could still be deleted or leaked.

Phishing, Email Scams, Invoice Manipulation

- ➔ A successful phishing attack can lead to fraudulent transfer of funds.
- ➔ Cybercriminals might manipulate email or phone systems and lead you or your staff to pay fake invoices.

Cyber Insurance

The provided financial protection is classified into:

First-Party Coverages

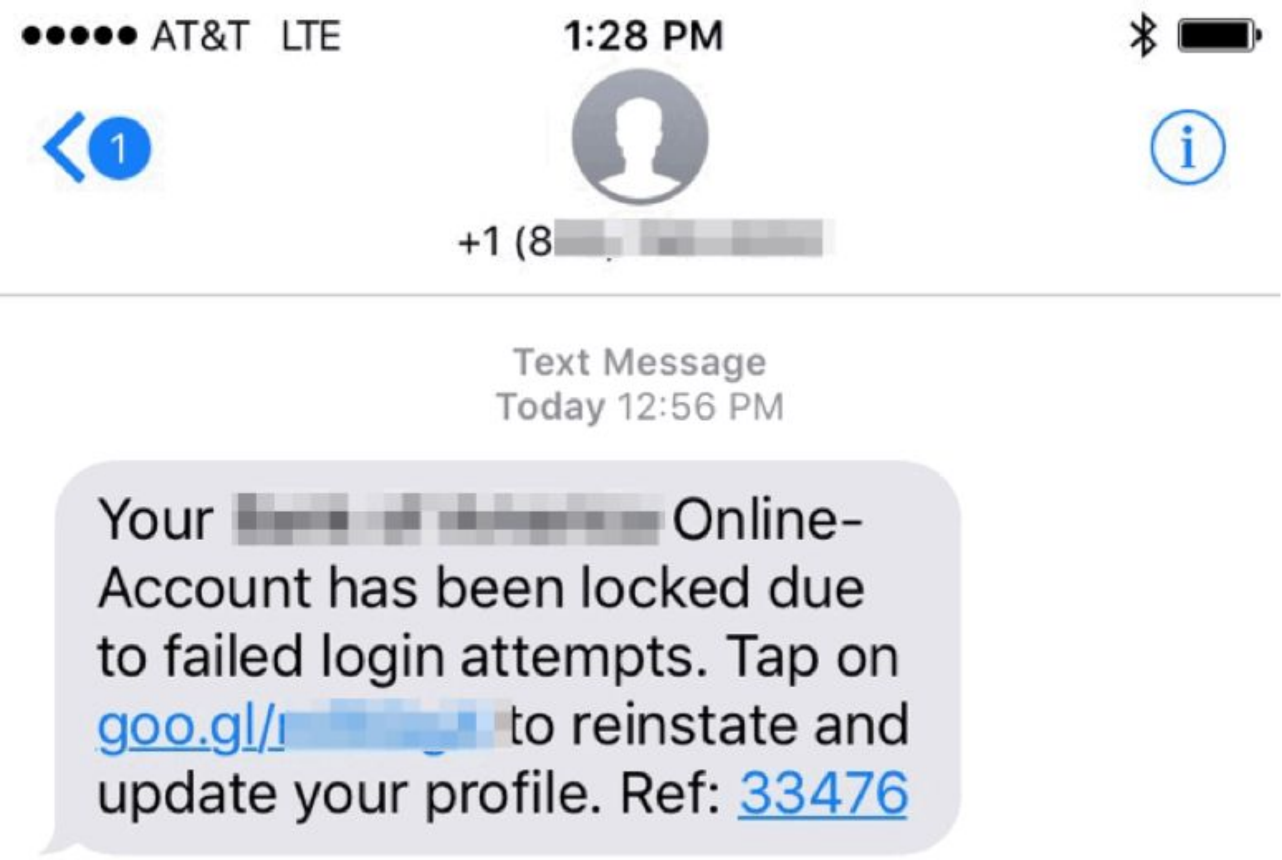
Coverage for the loss or damages sustained and for expenses to return to normal operations.

- Cybercrime
- Business Interruption
- Ransom payment
- Breach Notification/ Investigation costs
- Reputational harm
  - PR/Crisis Management

Third-Party Coverages

Expenses related to the monetary damages the insured becomes legally obligated to pay.

- Lawsuits from vendors or clients
- Fines & penalties from Regulatory bodies
- PCI Fines and Penalties



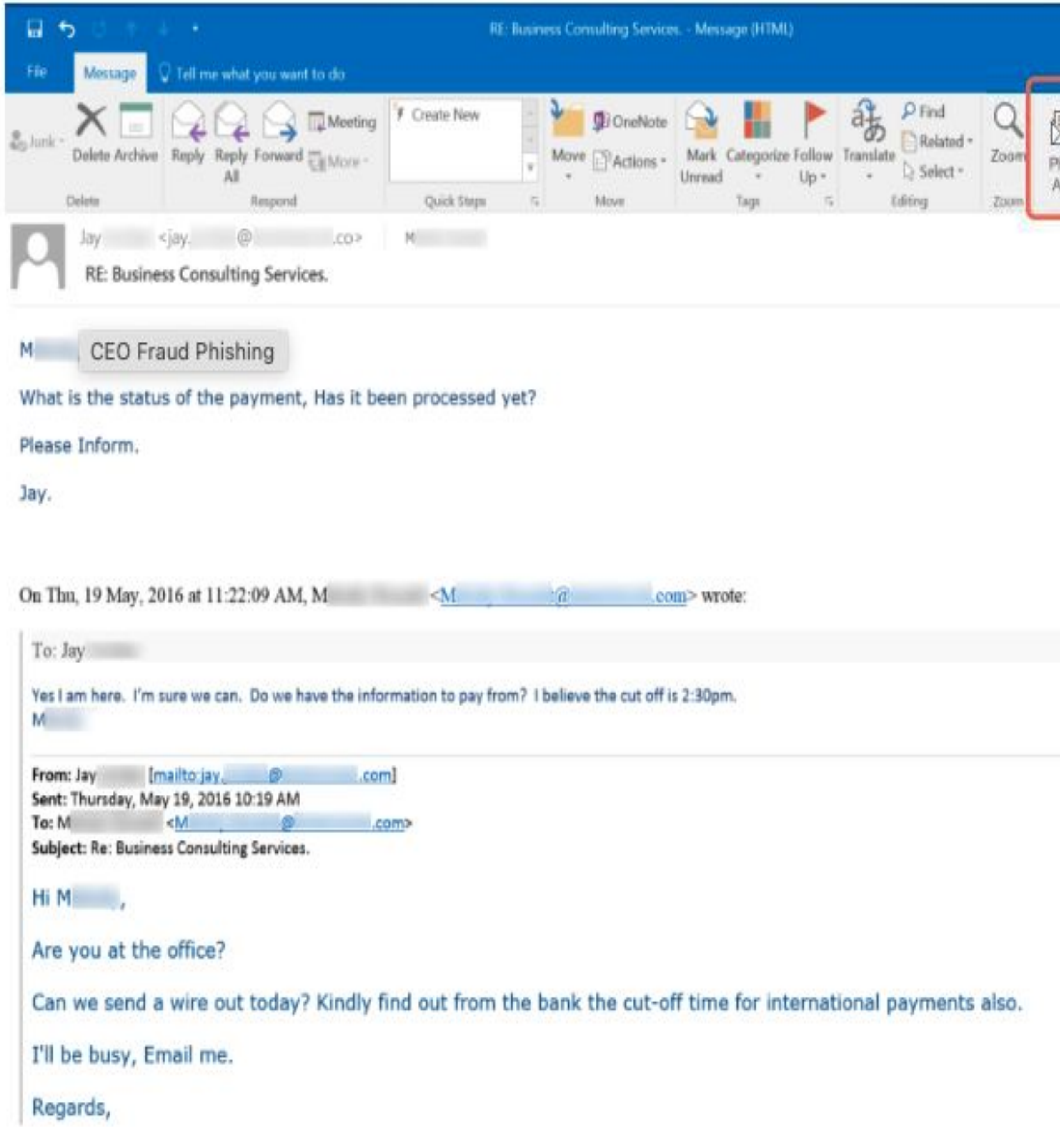
Your [redacted] Online-Account has been locked due to failed login attempts. Tap on goo.gl/[redacted] to reinstate and update your profile. Ref: 33476

Cyber Crime looks like..

Phishing/ Smishing/Vishing

Fake emails, texts, or calls from bad actors pretending to be legitimate in order to steal sensitive data.

- Avoid phishing attacks by **not reacting impulsively and always verifying the source of an email.** Watch out for:
    - Poorly written emails/spelling errors in the body of the message
    - Unfamiliar senders
    - A sense of urgency with a suspicious link attached to “resolve” the issue.
    - An unusual request
    - Inconsistencies
    - Subtle threats
    - Too good to be true emails



Jay [redacted] <jay.[redacted]@[redacted].co> M[redacted]

RE: Business Consulting Services.

M[redacted] CEO Fraud Phishing

What is the status of the payment, Has it been processed yet?

Please Inform.

Jay.

On Thu, 19 May, 2016 at 11:22:09 AM, M[redacted] <M[redacted]@[redacted].com> wrote:

To: Jay[redacted]

Yes I am here. I'm sure we can. Do we have the information to pay from? I believe the cut off is 2:30pm.
M[redacted]

From: Jay[redacted] [mailto:jay.[redacted]@[redacted].com]
Sent: Thursday, May 19, 2016 10:19 AM
To: M[redacted] <M[redacted]@[redacted].com>
Subject: Re: Business Consulting Services.

Hi M[redacted],

Are you at the office?

Can we send a wire out today? Kindly find out from the bank the cut-off time for international payments also.

I'll be busy, Email me.

Regards,

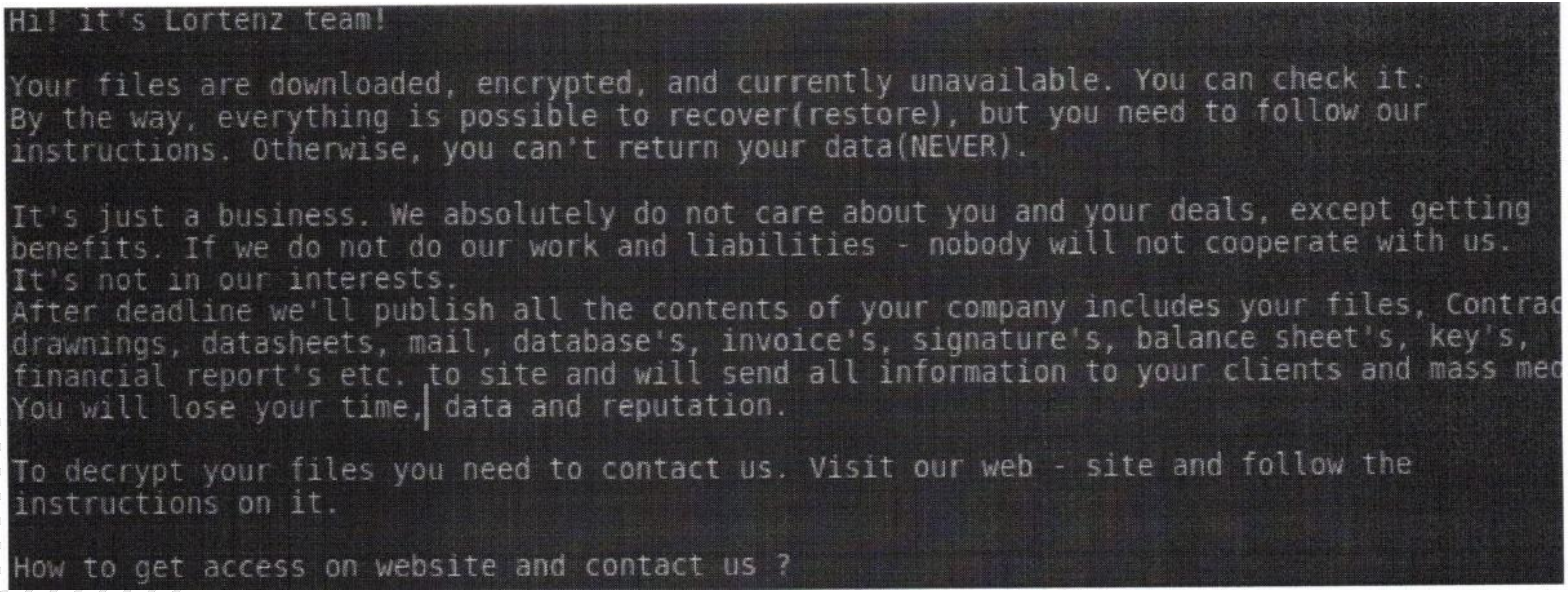
Cyber Crime looks like..

Social Engineering

The malicious act of obtaining confidential information through manipulation.

- This usually takes the form of invoice manipulation or wire fraud.
- Avoid social engineering attacks by not opening emails and attachments from suspicious sources, double-checking requests and implementing Multi-Factor Authentication.

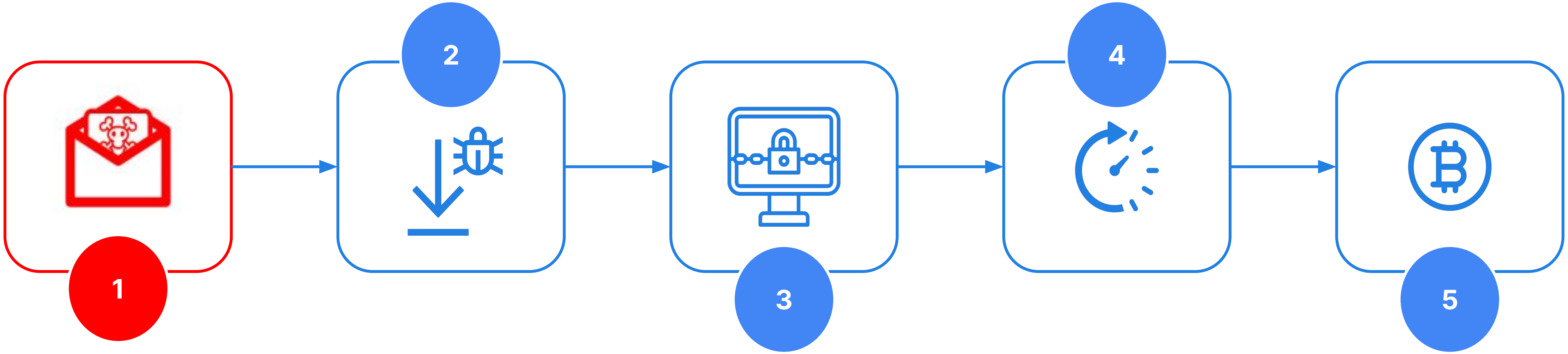
Sample Ransom Note



```
Hi! it's Lortenz team!

Your files are downloaded, encrypted, and currently unavailable. You can check it.
By the way, everything is possible to recover(restore), but you need to follow our
instructions. Otherwise, you can't return your data(NEVER).

It's just a business. We absolutely do not care about you and your deals, except getting
benefits. If we do not do our work and liabilities - nobody will not cooperate with us.
It's not in our interests.
After deadline we'll publish all the contents of your company includes your files, Contrac
drawnings, datasheets, mail, database's, invoice's, signature's, balance sheet's, key's,
financial report's etc. to site and will send all information to your clients and mass med
You will lose your time, data and reputation.

To decrypt your files you need to contact us. Visit our web - site and follow the
instructions on it.

How to get access on website and contact us ?
```

Anatomy of a Ransomware Through Email Phishing

One click on a bad email can lead to a million dollar ransomware attack.



One employee clicks on a malicious link in phishing email

Malicious code is downloaded and spreads across network

The malicious code encrypts files and data across network

Victim receives a ransom demands
and deadline to pay it.

Victim needs to pay ransom (Bitcoin or other) to regain access to systems

The Cost of Ransomware

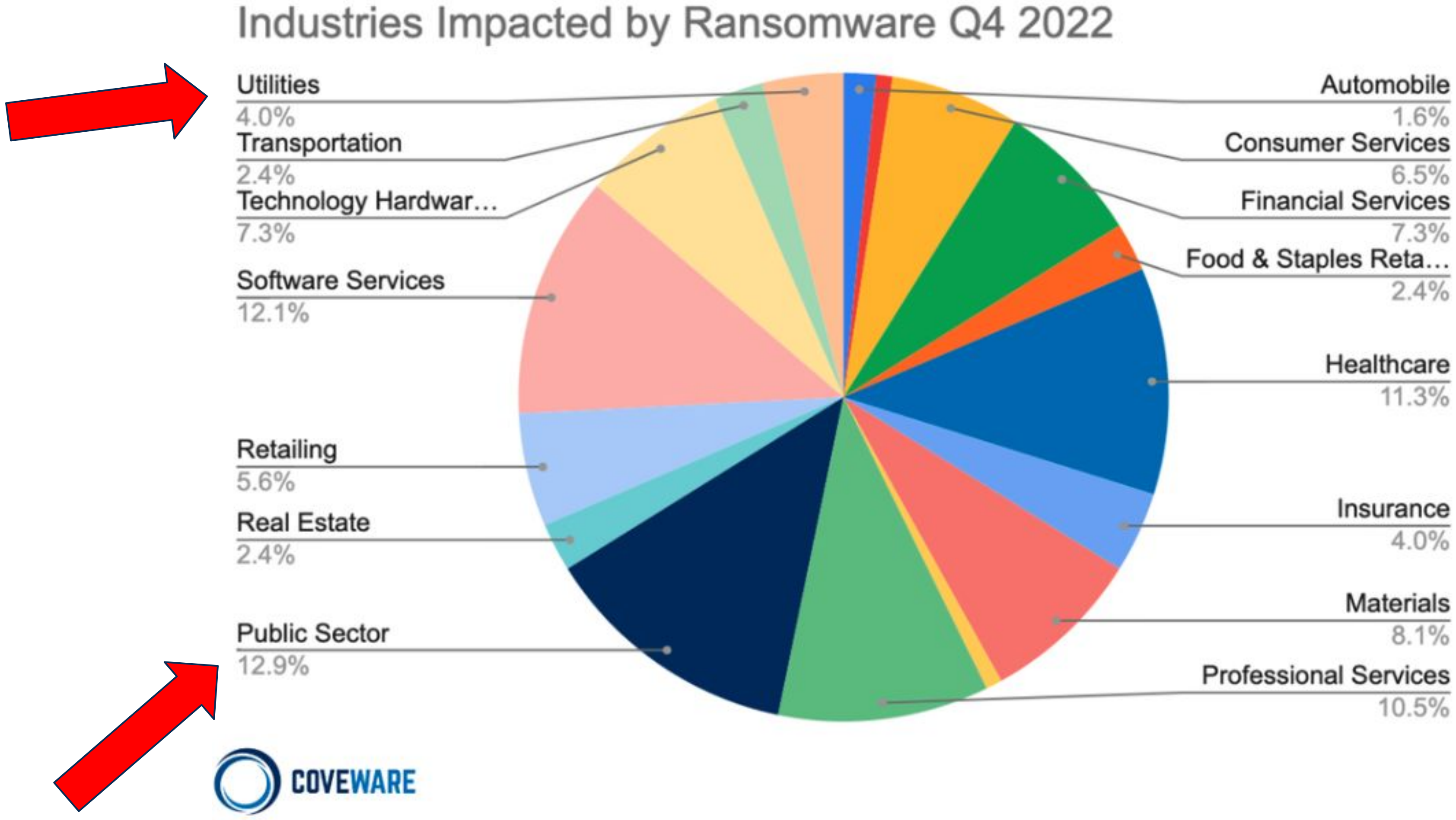
$570,000 – $812,360 (avg. ransom)

$1,400,000 (avg. recovery cost)

$2,200,000 (total cost)

for every SME hit by ransomware in the last five years

No Industry is Immune to Ransomware Attacks



Source:
https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments

Ransomware - an Epidemic for SMEs

82%

of ransomware targets are small business

80%

of victims are hit a second time

47%

of small businesses with less than 50 employees have no resources for cybersecurity

Why Standalone Cyber?

For better protection

LIMITS & COVERAGES DEDICATED TO CYBER

COWBELL STANDALONE POLICIES

- ✓ 1st and 3rd party coverage
- ✓ Cyber crime
- ✓ Ransomware
- ✓ Business Interruption
- ✓ Wide range of limit/deductible options

What to look for in a cyber insurance policy

1. Clarity of coverage and ease/ automation of process

2. Customization (industry and individual accounts)

3. Transparency with Cyber Risk Assessment

4. Value-Add Services:

- ■ Cyber risk assessment and benchmarking
- ■ Services for improvement of cyber risk profile
- ■ Expert services (pre & post)
- ■ Cyber Awareness Training

Pool/ Packaged vs Standalone Cyber

Major Policy Differentiators

Scope of Coverage

- ***Pool/Packaged*** policies are often limited to data breach incidents.
- ***Standalone*** policies offer broader coverage as the whole policy is specific to Cyber insurance.

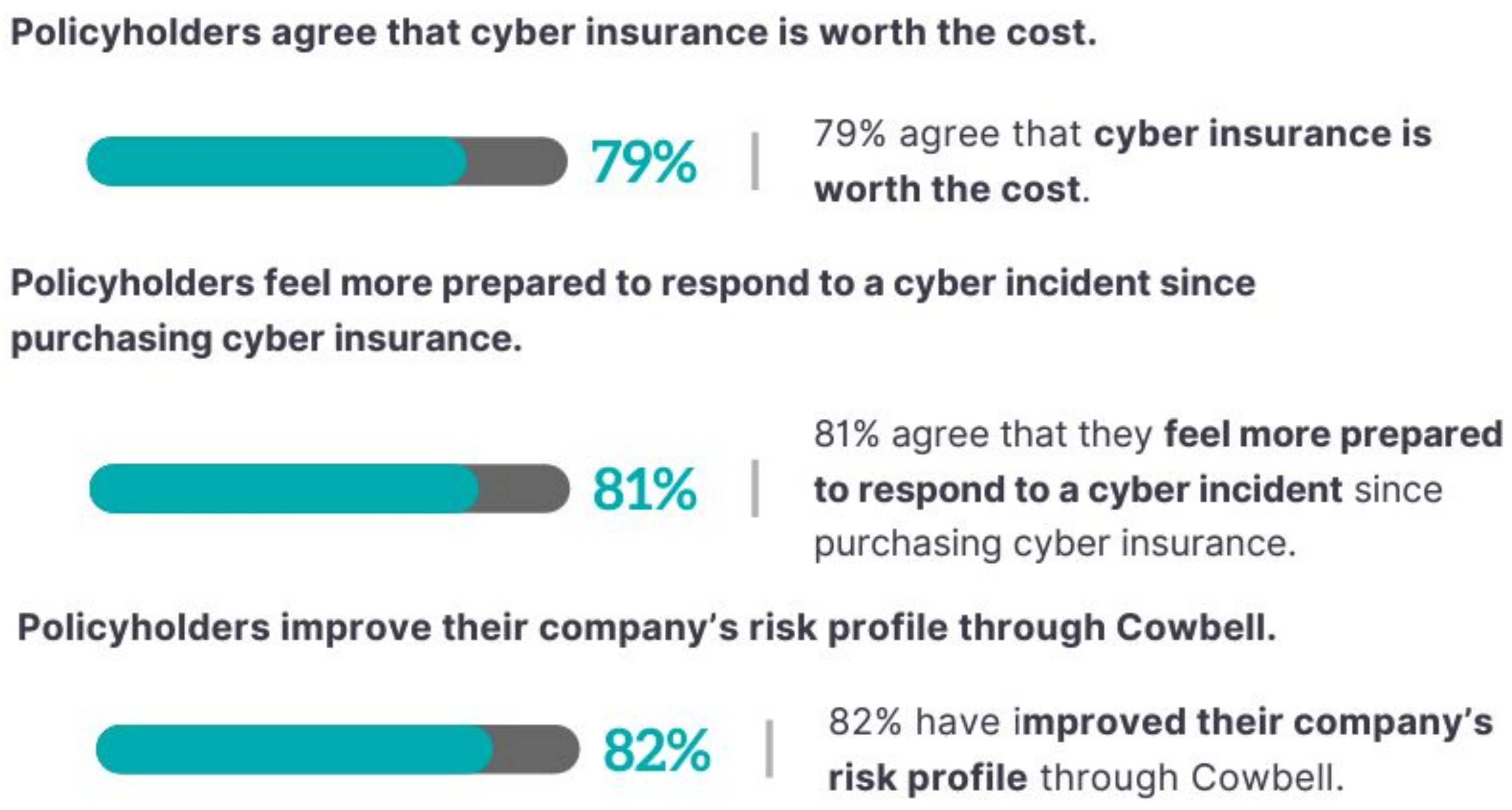
Coverage Limits

- ***Pool/Packaged*** policies limits are often sub-limited and too low to cover most cyber incidents.
- ***Standalone*** policies are dedicated to cyber incidents and have coverage limits up to $15 million.

Claim Resources

- ***Pool/Packaged*** policies claims teams are generalists when it comes to dealing with cyber incidents.
- ***Standalone*** policies offer cyber claims specialists in the event of a cyber incident.

2022 Policyholder Perspective



Policyholders agree that cyber insurance is worth the cost.

79%

79% agree that **cyber insurance is worth the cost**.

Policyholders feel more prepared to respond to a cyber incident since purchasing cyber insurance.

81%

81% agree that they **feel more prepared to respond to a cyber incident** since purchasing cyber insurance.

Policyholders improve their company's risk profile through Cowbell.

82%

82% have **improved their company's risk profile** through Cowbell.

The Cowbell Difference

Cowbell Approach

Traditional insurance companies versus the Cowbell approach

Insurability Gaps

- Inadequate limits
- Many risks not covered
- Ever changing cyber risks

Relevant Coverages

- Dedicated stand-alone cyber insurance
- Policy terms aligned to your needs
- Limits dedicated to cyber

Coverage Confusion

- Lengthy, manual process
- Data is unverifiable
- Binding delays

Clear Understanding

- Digital, simplified application process
- Unbiased, verifiable data
- Policy with value on day 1

Complexity

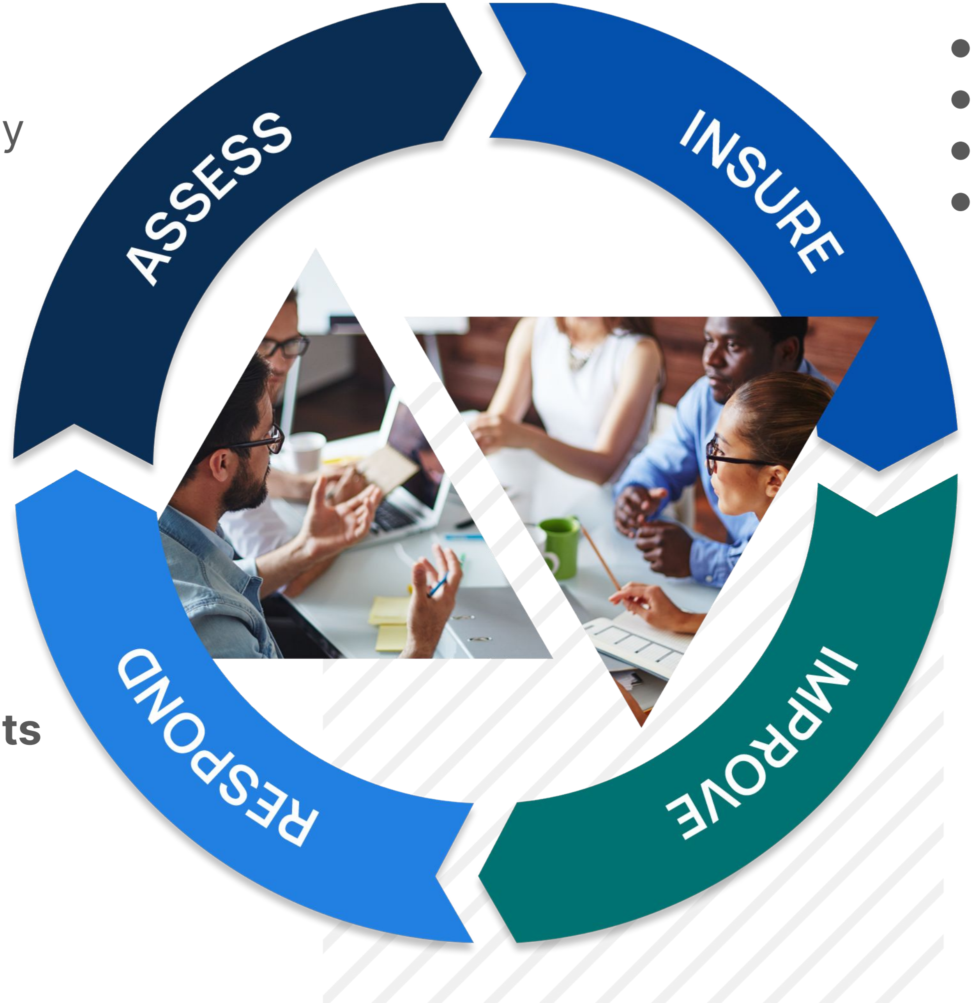
- Inconsistent, opaque coverages
- Policy disconnected from risk
- One-size fits all model

5 min. Quote-to-Issue

- Easy to understand coverages
- Coverages that match your risk profile
- Continuous risk assessment

Closed-loop risk management

- Identify assets
- Validate configuration for security
- Validate security controls and processes
- **Identify and understand risk exposures**



- Transfer risks
- Plan response
- Plan recovery
- Identify internal/external resources

- Improve security controls
- Test incident response plans
- Implement learnings
- Train employees on cybersecurity
- Take advantage of marketplace resources (Cowbell Rx)

- 24/7 breach hotline
- **In-house cyber claims experts**
- Financial Resources
- Forensic Investigators
- Ransom Negotiators

Bundled Risk Management Services

1) Risk Engineering Services

- Live sessions with cyber risk engineers throughout the policy lifecycle.
- Address subjectivities, understand and mitigate risk exposures.

riskengineering@cowbellcyber.ai

2) In-house Cyber Claims Experts

- Claims experts deliver better outcomes with faster recovery time and lower severity.
- Our experienced ransom negotiators have reduced payments by 70%.

claims@cowbellcyber.ai

3) Cybersecurity Awareness Training

- Free training for up to 20 employees with our partner, Wizer, a $400 value per year.
- Employee training reduces the cost of phishing by more than 50%.

Learn more

4) Password Management

- Free 6-month subscription to Business Password Manager provided by NordPass.
- Unlimited employee licenses. For a company of 100 users this is a cost savings of over $1200.

partners@cowbellcyber.ai for activation code

5) Rx Marketplace

- Industry leading cybersecurity products and services that are vetted, discounted, and customized for Cowbell policyholders.

cowbell.insure/rx/

6) Deeper Insights with Connectors

- New and renewing Prime 250 policyholders get a 5% premium credit by easily integrating with commonly used cyber tools and technologies.

cowbell.insure/cowbell-connectors/

Cowbell 365:

24x7x365 Cyber Claims and Risk Management Services

cowbell®

What is Cowbell 365?

Cyber claims specialists and cyber risk engineers bringing expertise and responsiveness 24×7×365

The team behind every policy:

- ❏ Cyber claims counsel and specialists,
- ❏ Operations team dedicated to swift payments and claims processing;
- ❏ Best-in-class incident response vendors;
- ❏ Risk engineers monitoring the threat landscape;
- ❏ Risk engineers assisting insureds in adopting cybersecurity best practices.

Mission

Lower Incident Frequency and Severity

When improving their cyber hygiene, policyholders can **drastically and easily** reduce their cyber risk. If they are more secure than industry peers, the chances of a successful attack are low.

Full Transparency at Renewal

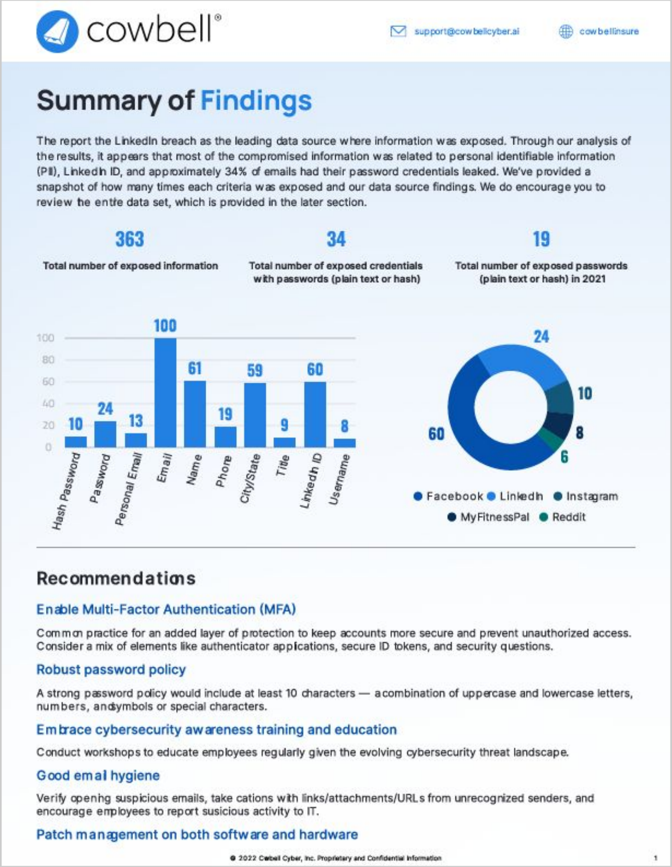
Good cyber practices will positively impact your clients’ cyber renewals, and their premium.

Risk Engineering Services

1. Addressing Subjectivities
2. Risk Assessment / Renewal
3. Spotlight & Risk management resources
4. Post-claim assessment

Risk Management Services

Dark Web Reports



cowbell®

support@cowbellcyber.ai

cowbellinsure

Summary of Findings

The report the LinkedIn breach as the leading data source where information was exposed. Through our analysis of the results, it appears that most of the compromised information was related to personal identifiable information (PII), LinkedIn ID, and approximately 34% of emails had their password credentials leaked. We've provided a snapshot of how many times each criteria was exposed and our data source findings. We do encourage you to review the entire data set, which is provided in the later section.

363	34	19
Total number of exposed information	Total number of exposed credentials with passwords (plain text or hash)	Total number of exposed passwords (plain text or hash) in 2021

Recommendations

Enable Multi-Factor Authentication (MFA)

Common practice for an added layer of protection to keep accounts more secure and prevent unauthorized access. Consider a mix of elements like authenticator applications, secure ID tokens, and security questions.

Robust password policy

A strong password policy would include at least 10 characters — a combination of uppercase and lowercase letters, numbers, and symbols or special characters.

Embrace cybersecurity awareness training and education

Conduct workshops to educate employees regularly given the evolving cybersecurity threat landscape.

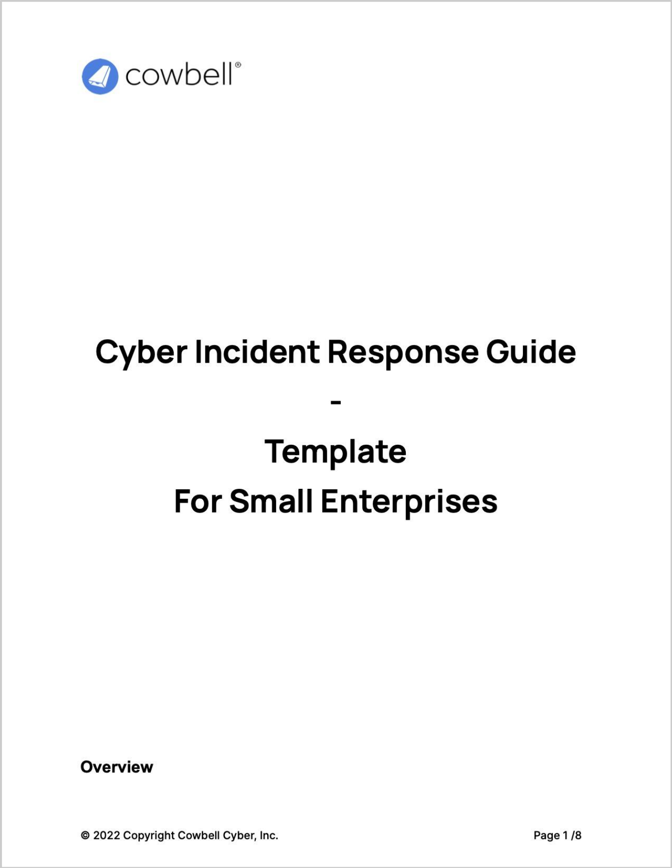
Good email hygiene

Verify opening suspicious emails, take cations with links/attachments/URLs from unrecognized senders, and encourage employees to report susicious activity to IT.

Patch management on both software and hardware

© 2022 Cowbell Cyber, Inc. Proprietary and Confidential Information 1

Free Templates



cowbell®

Cyber Incident Response Guide

-

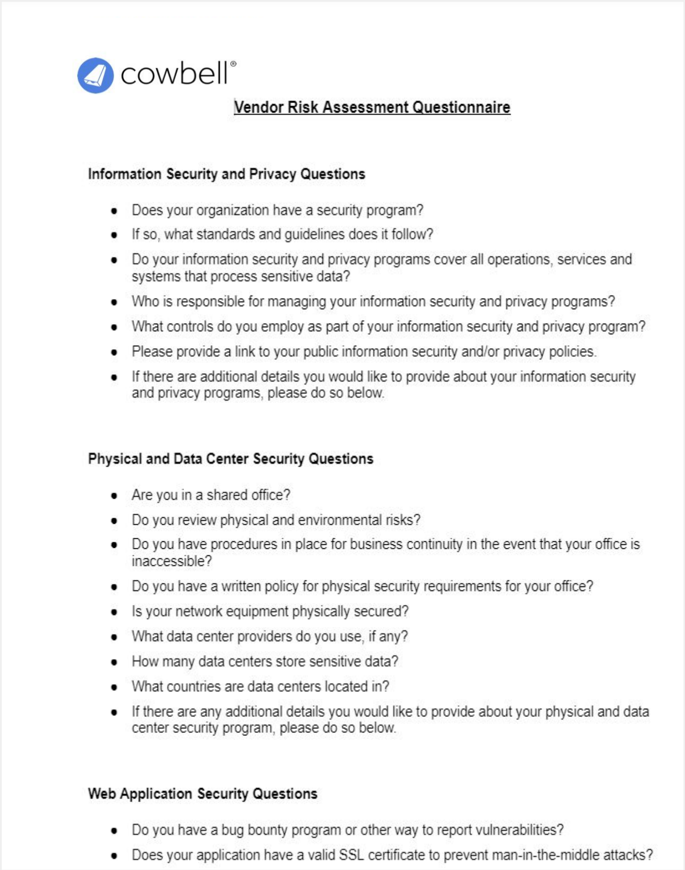
Template

For Small Enterprises

Overview

© 2022 Copyright Cowbell Cyber, Inc. Page 1 /8

Third Party Vendor Risk Assessment



cowbell®

Vendor Risk Assessment Questionnaire

Information Security and Privacy Questions

- Does your organization have a security program?
- If so, what standards and guidelines does it follow?
- Do your information security and privacy programs cover all operations, services and systems that process sensitive data?
- Who is responsible for managing your information security and privacy programs?
- What controls do you employ as part of your information security and privacy program?
- Please provide a link to your public information security and/or privacy policies.
- If there are additional details you would like to provide about your information security and privacy programs, please do so below.

Physical and Data Center Security Questions

- Are you in a shared office?
- Do you review physical and environmental risks?
- Do you have procedures in place for business continuity in the event that your office is inaccessible?
- Do you have a written policy for physical security requirements for your office?
- Is your network equipment physically secured?
- What data center providers do you use, if any?
- How many data centers store sensitive data?
- What countries are data centers located in?
- If there are any additional details you would like to provide about your physical and data center security program, please do so below.

Web Application Security Questions

- Do you have a bug bounty program or other way to report vulnerabilities?
- Does your application have a valid SSL certificate to prevent man-in-the-middle attacks?

cowbell®

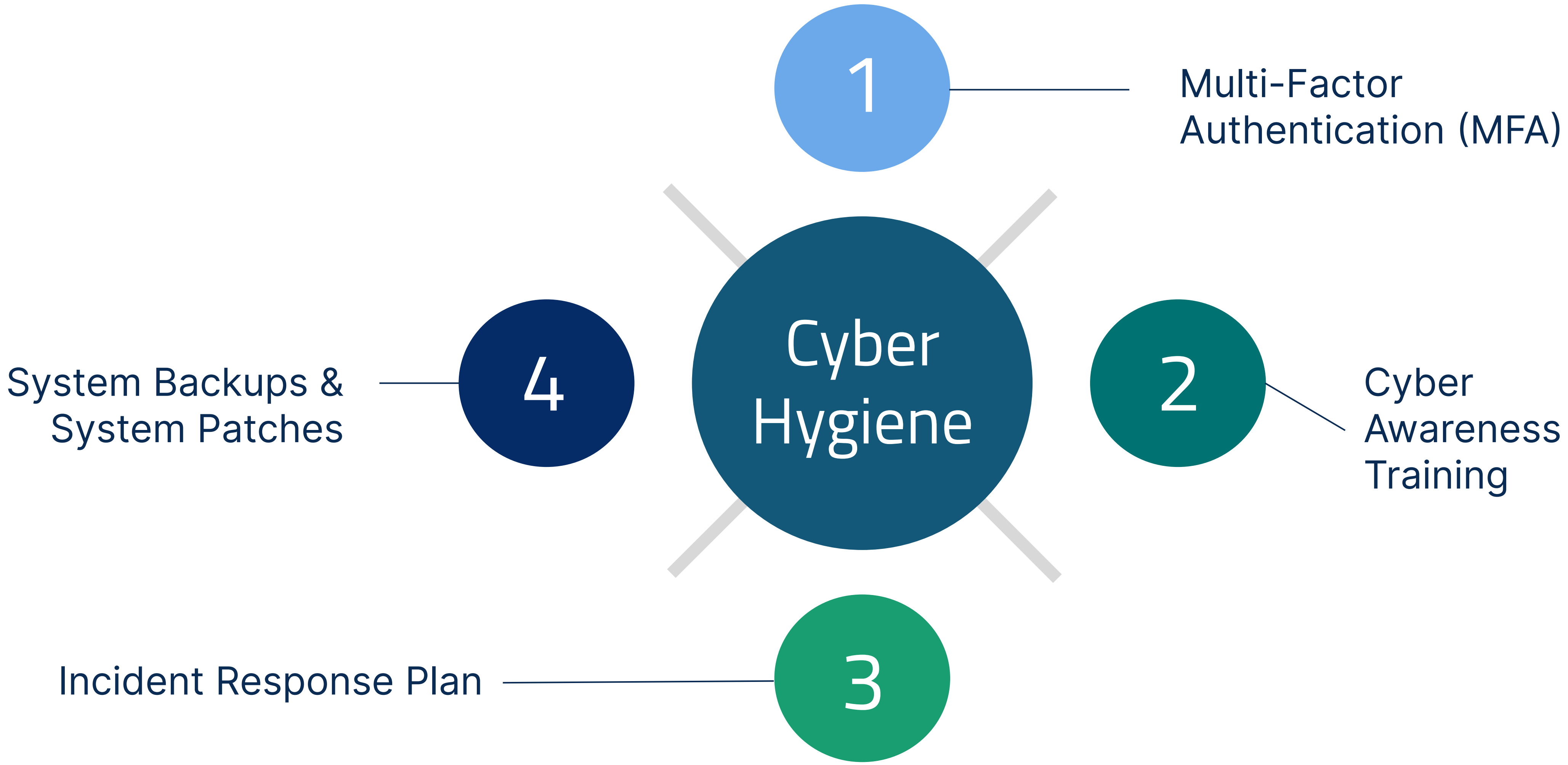
Risk Mitigation

Best Practices

cowbell®

Cyber Hygiene Overview

Best defence against cyber incidents



Cyber Hygiene

1 Multi-Factor Authentication (MFA)

2 Cyber Awareness Training

3 Incident Response Plan

4 System Backups & System Patches

Multi-Factor Authentication

When a user is required to provide two or more pieces of evidence to verify their identity in order to gain access to an app or digital resource.

- Easily implemented and mostly free of charge
- Available on most cloud service platforms
- Can be enforced centrally by account admins most of the time

Cyber Awareness Training

Employees are the first line of defense against many types of cyber incidents.

- Training to recognize and report malicious activities is the easiest and cheapest way of protecting business data and devices.

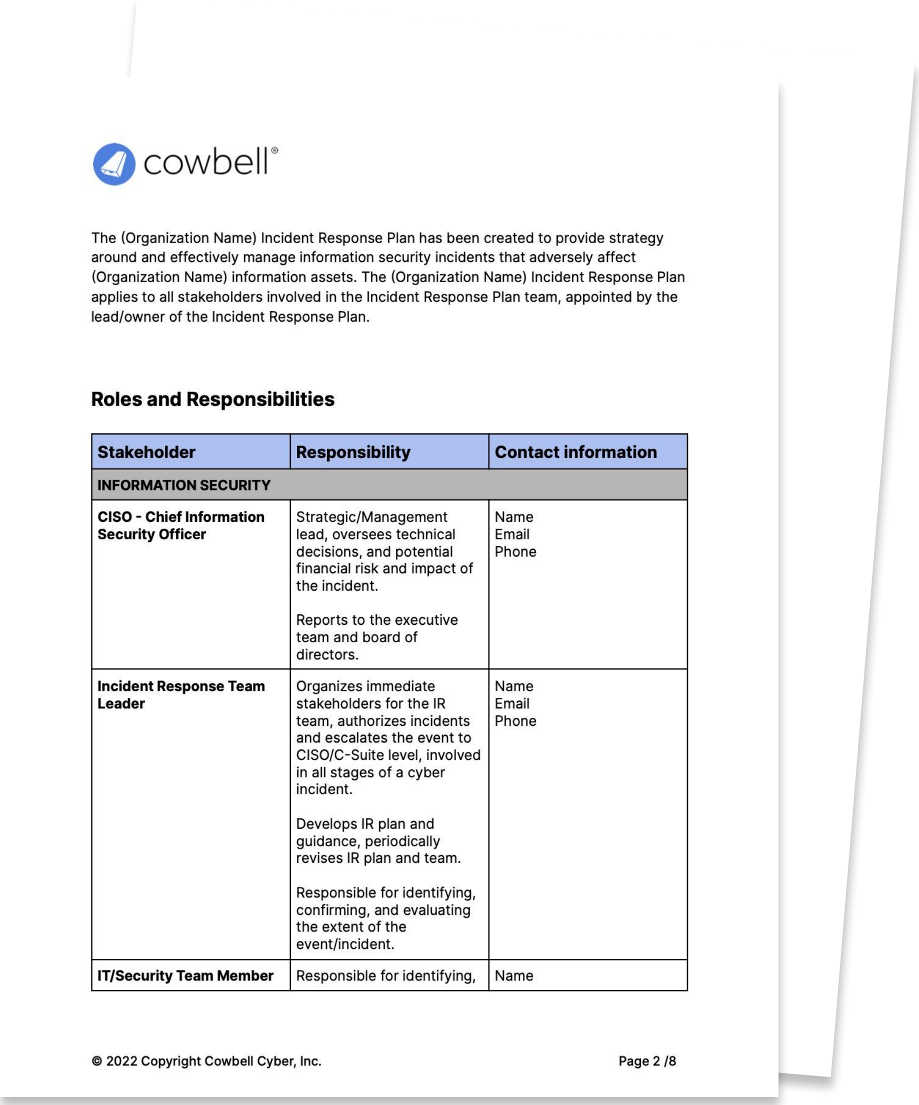
- 95% of surveyed professionals are still not able to recognize a phishing email. (source: Infosecurity UK)

- Cowbell policies include **20 employee seats to Wizer** cyber awareness training program

Incident Response Plan

Policyholders can customize and make it their own.

- Be prepared for times of crisis with who to call for help and what steps to take.
- The first 24 hours after an incident as been discovered as the most crucial for a faster recovery.
- A solid incident response plan can reduce the costs of a security incident by almost 50%.
- Cowbell provides an incident response template for policyholders. https://cowbell.insure/incident-response-plan/



cowbell®

The (Organization Name) Incident Response Plan has been created to provide strategy around and effectively manage information security incidents that adversely affect (Organization Name) information assets. The (Organization Name) Incident Response Plan applies to all stakeholders involved in the Incident Response Plan team, appointed by the lead/owner of the Incident Response Plan.

Roles and Responsibilities

Stakeholder	Responsibility	Contact information
INFORMATION SECURITY		
CISO - Chief Information Security Officer	Strategic/Management lead, oversees technical decisions, and potential financial risk and impact of the incident. Reports to the executive team and board of directors.	Name Email Phone
Incident Response Team Leader	Organizes immediate stakeholders for the IR team, authorizes incidents and escalates the event to CISO/C-Suite level, involved in all stages of a cyber incident. Develops IR plan and guidance, periodically revises IR plan and team. Responsible for identifying, confirming, and evaluating the extent of the event/incident.	Name Email Phone
IT/Security Team Member	Responsible for identifying,	Name

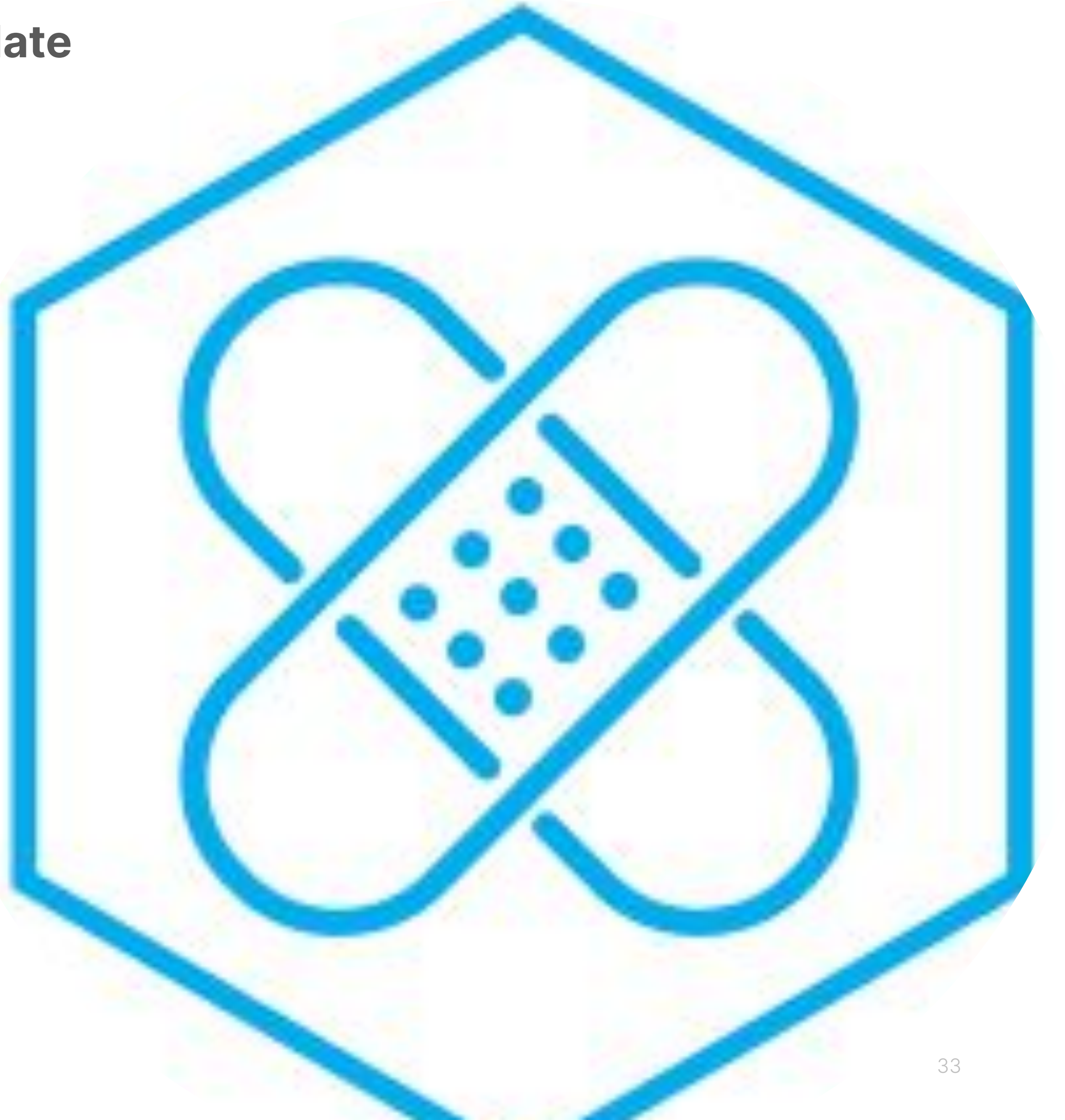
© 2022 Copyright Cowbell Cyber, Inc.

Page 2 /8

System Patches

Keeping devices, applications and website tools up to date with the most recent versions of software.

- Software that's not kept up to date is a known cause of cyber incidents
- Updates generally address security vulnerabilities within a program or product
- Threat actors exploit network weaknesses in older unpatched systems



System Backups

Recent backups can remove the necessity of paying a ransom

- Backups give the breach coach options and power when negotiating a ransom.
- It should be conducted at least on a monthly basis, ideally on a daily basis.
- Important backups should be stored on a Drive not connected to the Internet (the cloud).

What To Do When a Cyber Incident Happens

1. **Do not** attempt to resolve the issue on your own.
2. Report to Cowbell at (833) 633 – 8666 / cyber carrier
3. Develop a summary or timeline of events leading to the discovery of the cyber event.
4. Track all costs, if any, that might have incurred to date associated with the cyber event.

More details available to all on our website:

https://cowbell.insure >> Resource Tab

Check out the Cowbell Factors™ Podcast!

with host

Alexis Cierra Vaughn

AVP of Agency Marketing

alexis@cowbellcyber.ai

AVAILABLE ON ALL PODCAST STREAMING PLATFORMS!

Spotify

Listen on Apple Podcasts

iHeart

Listen on Google Podcasts

Learn More About Cyber Insurance

LEARNING MADE EASY
Cowbell Cyber Special Edition
Cyber Insurance
for dummies
A Wiley Brand
Discover why you need cyber coverage
Review how coverage and claims work
Find out how to apply for coverage
Brought to you by
COWBELL CYBER
Steve Kaelble
concept of cyber insurance
COWBELL CYBER
ISBN: 978-1-119-83924-8
Not For Resale

As a thank you for attending, you will receive a free copy of the e-book.

cowbell®

THANK YOU!

Any questions?