Doing Business Securely

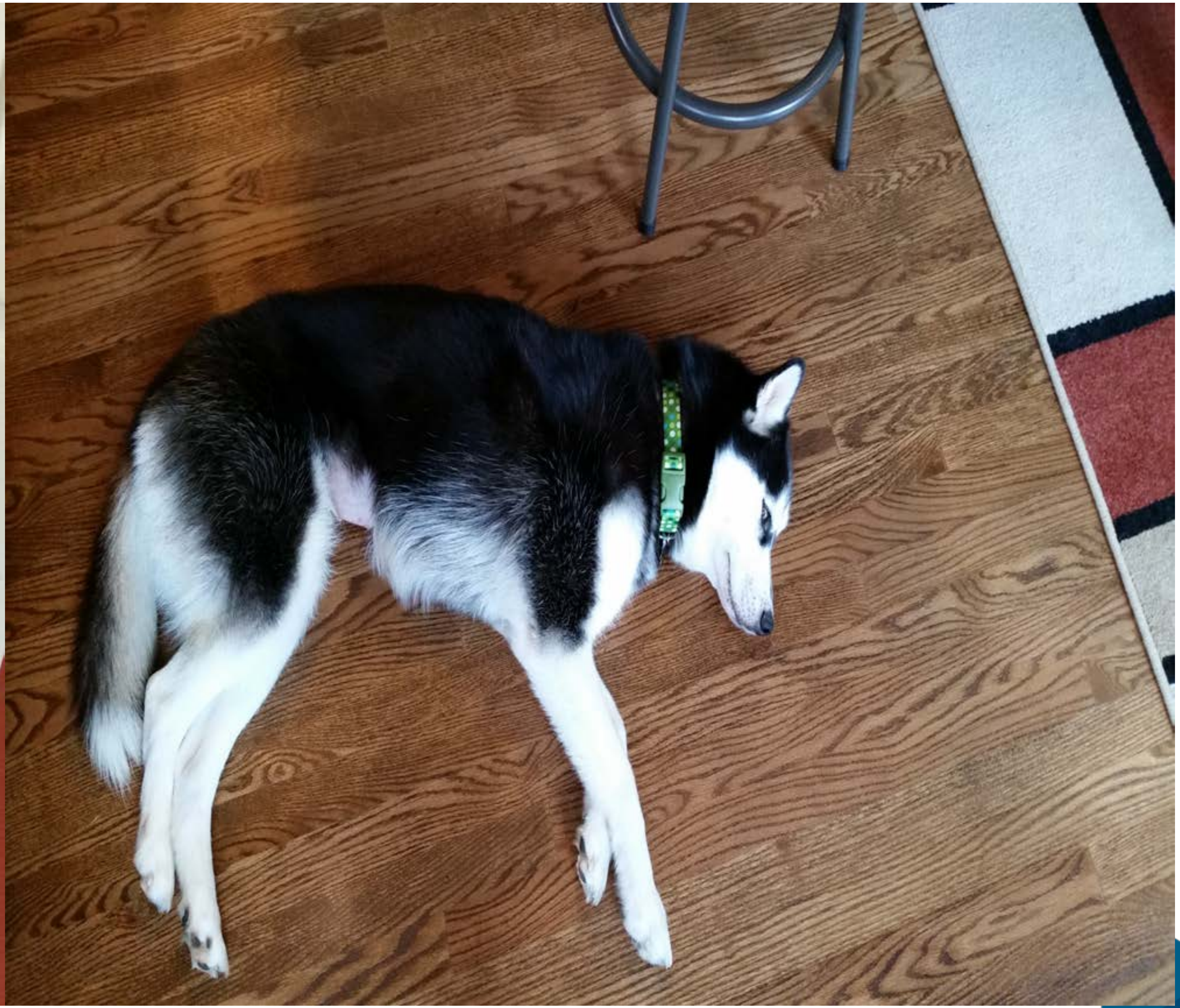
MBBA – Metro Chapter

January 3, 2019

Facilitated by John Holbel

President – CMIT Solutions of Ann Arbor, Plymouth, and Novi.

Live Repo



BIO – John Holbel (Novi Home)

- Wayne State University – B.S. Computer Science
- Hewlett-Packard – 10 Years (Software Development)
- Ernst & Young LLP – 5 Years (Technology Consulting)
- Ryder Logistics – 18 Years (IT Management)

- **Insane Customer Obsession**
  - Collaboration, Transparency, & Business Value

Small Business Owner – I understand small business

- Ran my own business within a business at Ryder and consultant to my internal customer base.
- Small offices, large office, warehouses, remote locations, remote data centers, on-premise & Cloud
- Greater than 1,500 end users, 3 Shift Operations, & 24x7 support
- Project Management Professional

- Need to be with customers & solve problems.

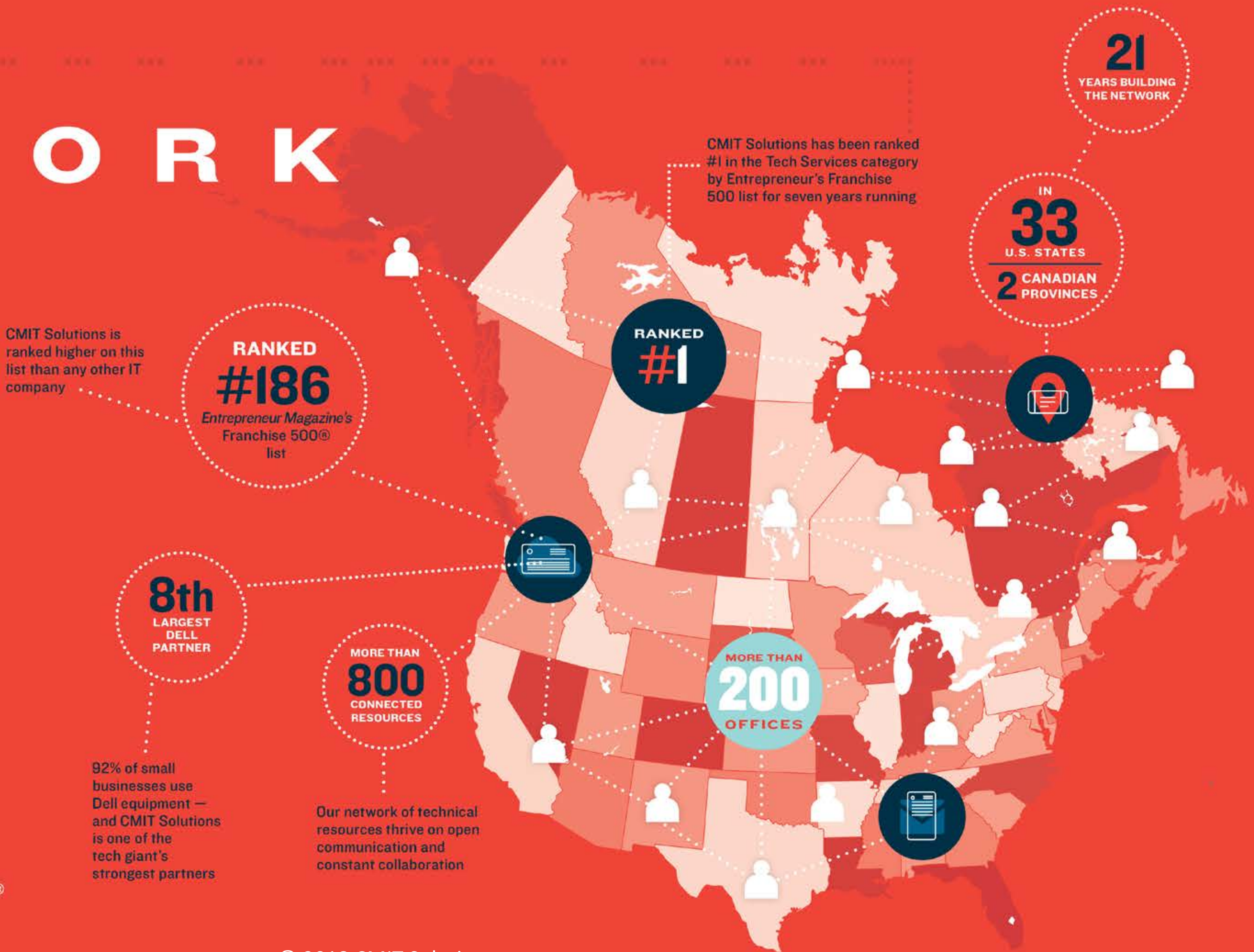
- **Bringing enterprise class services to the small business community.**
- HIPAA Training & Other **Regulatory Compliance**
  - Much to be leveraged across industries (security) & very exciting
  - Security expertise began in the software development world, DEVOPS. (A new forthcoming target of Hackers)
- **What does compliance mean to me?**
  - Simply put, compliance is a voyage, and a successful roadmap requires establishing “best efforts” and having the ability to show that they were relentlessly pursued.

THE CMIT NETWORK

How powerful is the CMIT Solutions network? Let's look at the big North American picture:

We provide right sized solutions for small to mid-size business.

We take care of the details so you can focus on your business.



21 YEARS BUILDING THE NETWORK

CMIT Solutions has been ranked #1 in the Tech Services category by Entrepreneur's Franchise 500 list for seven years running

IN 33 U.S. STATES 2 CANADIAN PROVINCES

RANKED #1

CMIT Solutions is ranked higher on this list than any other IT company

RANKED #186 *Entrepreneur Magazine's* Franchise 500® list

8th LARGEST DELL PARTNER

92% of small businesses use Dell equipment — and CMIT Solutions is one of the tech giant's strongest partners

MORE THAN 800 CONNECTED RESOURCES

Our network of technical resources thrive on open communication and constant collaboration

MORE THAN 200 OFFICES

CMIT Solutions® Your Technology Team

Doing Business Securely means

1.) Business Continuity - Disaster Recovery Planning
2.) Industrialized / Proven Backups
3.) Cyber Security
   - Cyber attacks can happen to anyone.
   - What are we trying to protect?
   - How much protection is needed?

Would you put a $ 10 fence around a $ 100 horse?

Does it make sense to put a $ 100 fence around a $ 10 horse?

For the right security, you need to know what your horse is worth.

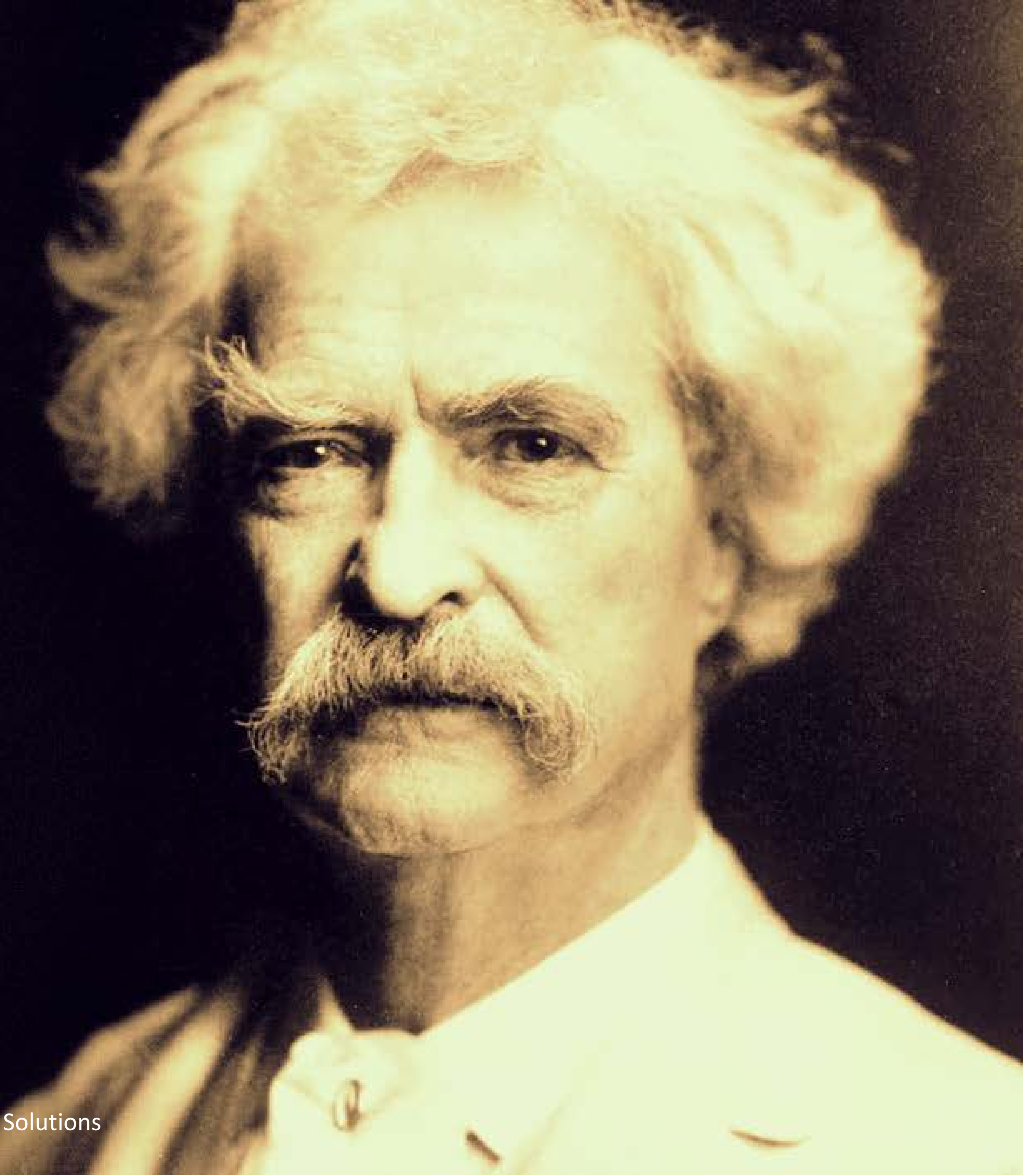
The same concepts apply to protecting your data. **What is your data worth?**

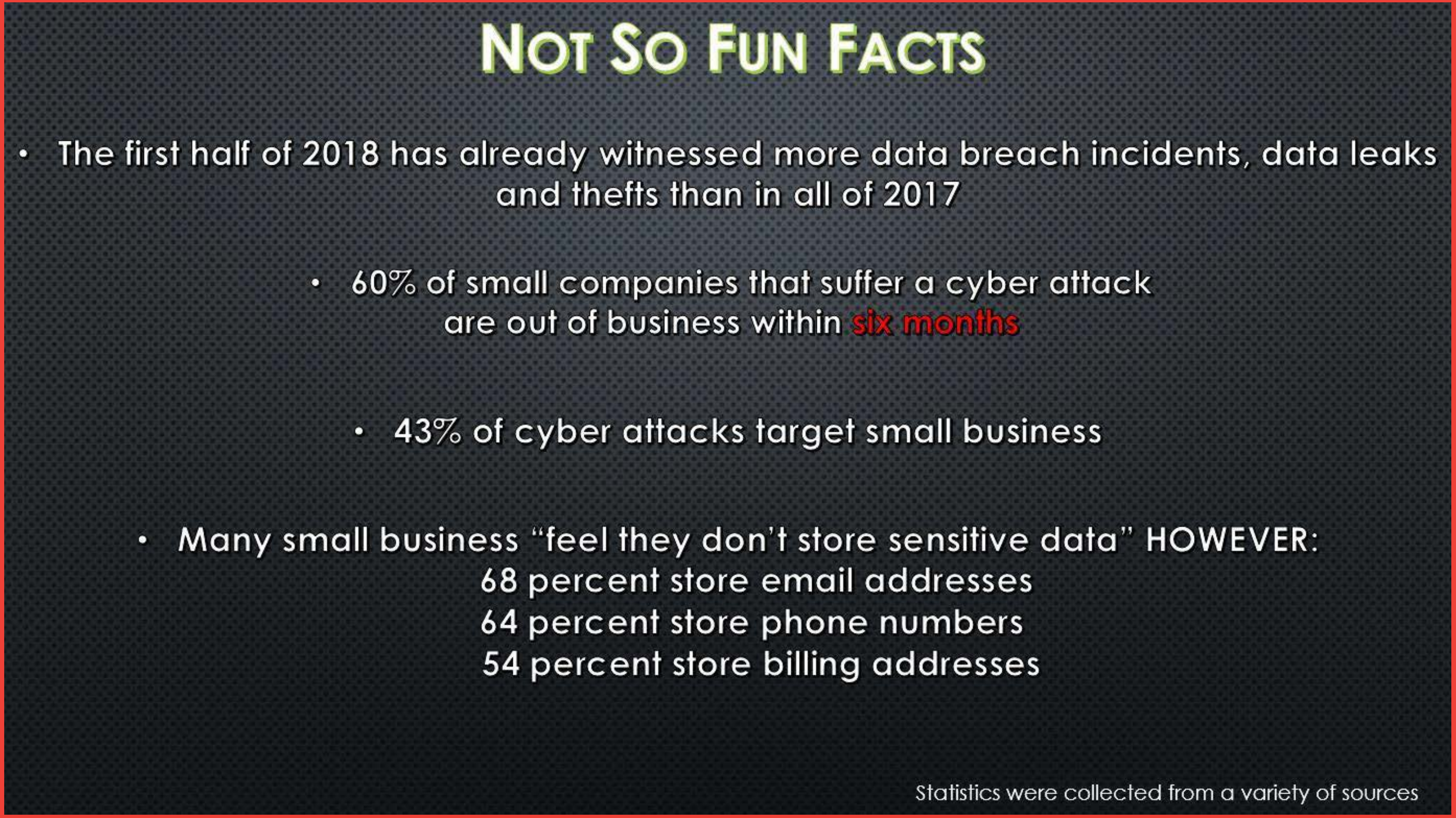
Raise Your Hand If…

1. You have experienced a cyber attack
2. You have a client that has
3. Know a business that has

“Get your facts first. Then you can distort them as you please.”

Mark Twain





Not So Fun Facts

- The first half of 2018 has already witnessed more data breach incidents, data leaks and thefts than in all of 2017

- 60% of small companies that suffer a cyber attack are out of business within six months

- 43% of cyber attacks target small business

- Many small business "feel they don't store sensitive data" HOWEVER:
  68 percent store email addresses
  64 percent store phone numbers
  54 percent store billing addresses

Statistics were collected from a variety of sources

Understanding The Next Wave Of Threats

- Facebook
- LinkedIn
- All Social Media
- The Hacking “Business” understands much more about your organization than you want to believe !!

Current Trends: Types of Attacks (a short list)

Malware/Viruses

Any “malicious software” designed to secretly access your computer

Phishing—(a type of Social Engineering)

Cybercriminals try to persuade you to give them sensitive information

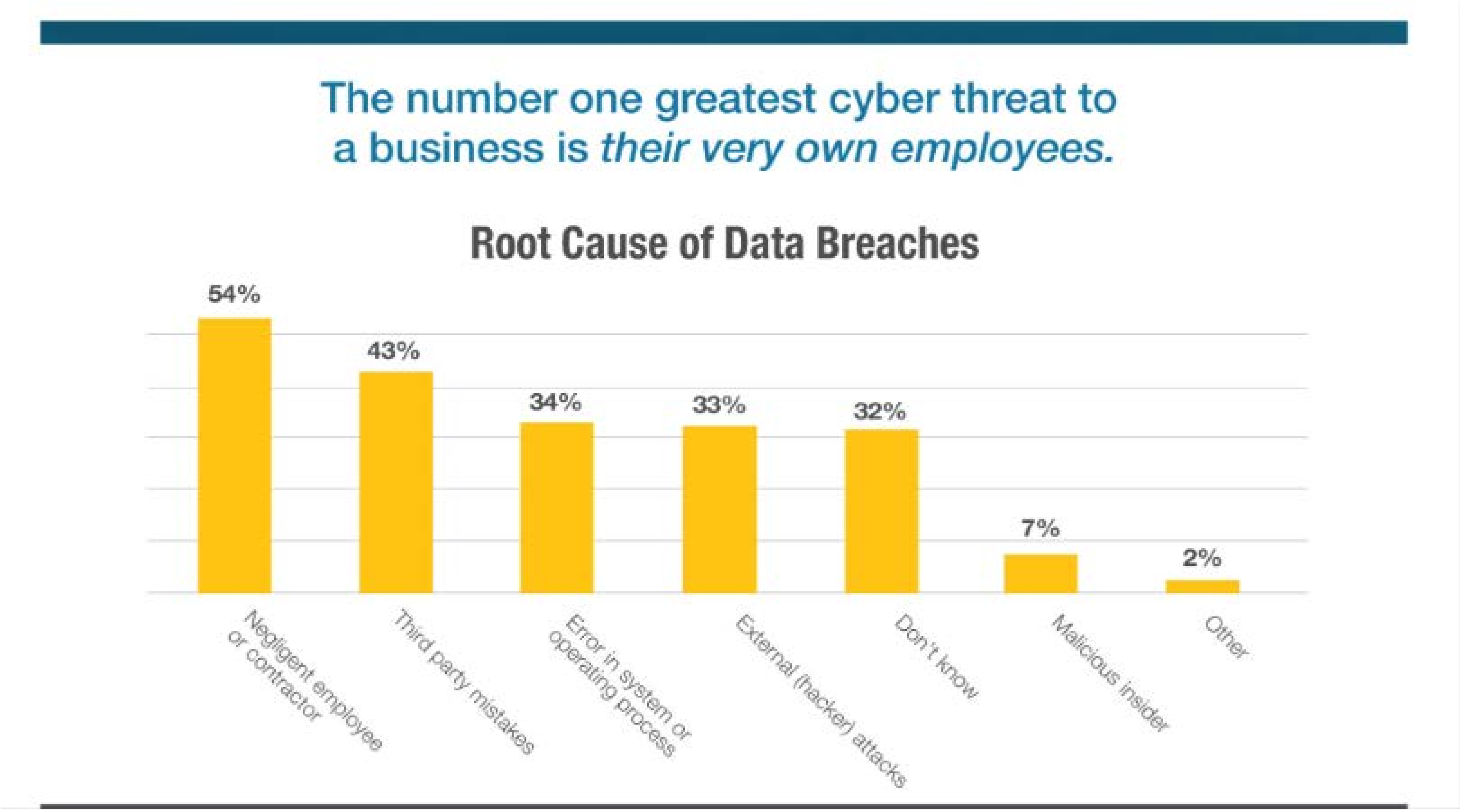
91% of attacks by cyber criminals start through phishing

Business Email Compromise (BEC)-Executive password theft via Dark Web. BEC attacks spoof trusted domains, imitate brands and/or mimic corporate identities. In many cases, the emails appear from a legitimate or trusted sender, or from the company CEO typically asking for wire transfers.

Ransomware

Malware that encrypts data or locks computers until a ransom is paid

2017 Ponemon Institute: State of Cyber Security



The number one greatest cyber threat to a business is *their very own employees.*

Probability of cyber attack or data breach

50%+ of small businesses have been breached in last 12 months

- Ponemon Institute: The 2017 State of SMB Cybersecurity

"There are only two types of companies: those that have been hacked, and those that will be."

- FBI Director Robert Mueller

Cyber Attacks can lead to Monetary Loss

It’s not a question of *if* but *when*

39% of organizations saw a substantial loss of revenue because of a cyber- attack.

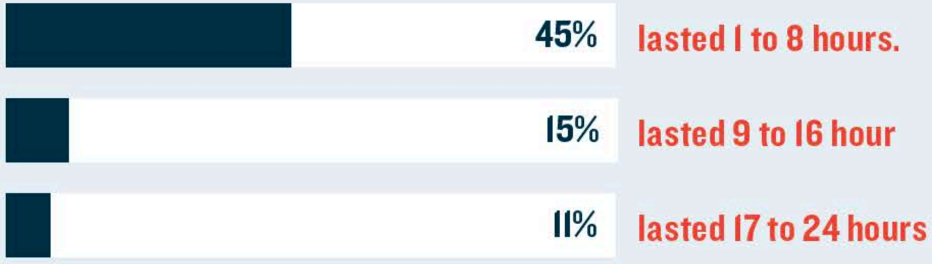
42% saw a business opportunity lost

39% saw a substantial loss of customers.

Source: Cisco 2017 Annual Cyber Security Report

An outage can shut down your business and lead to loss of productivity and income. Ensure outages are not an issue with the Cybersecurity Assessment.

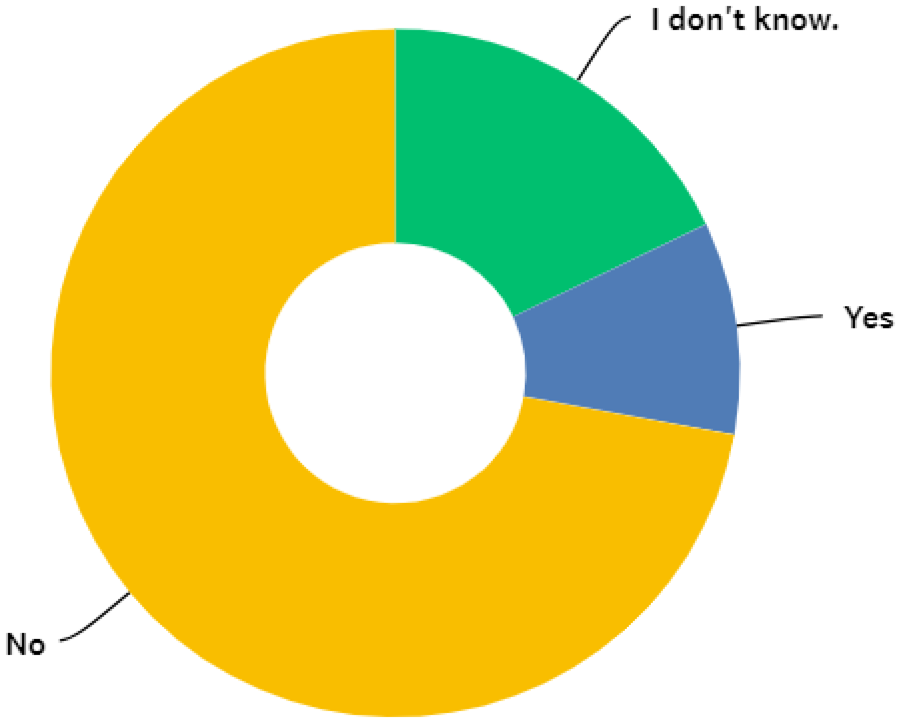
Network Outages that are caused by security breaches can often have a long-lasting impact.



Source: Cisco 2017 Security Capabilities Benchmark Study

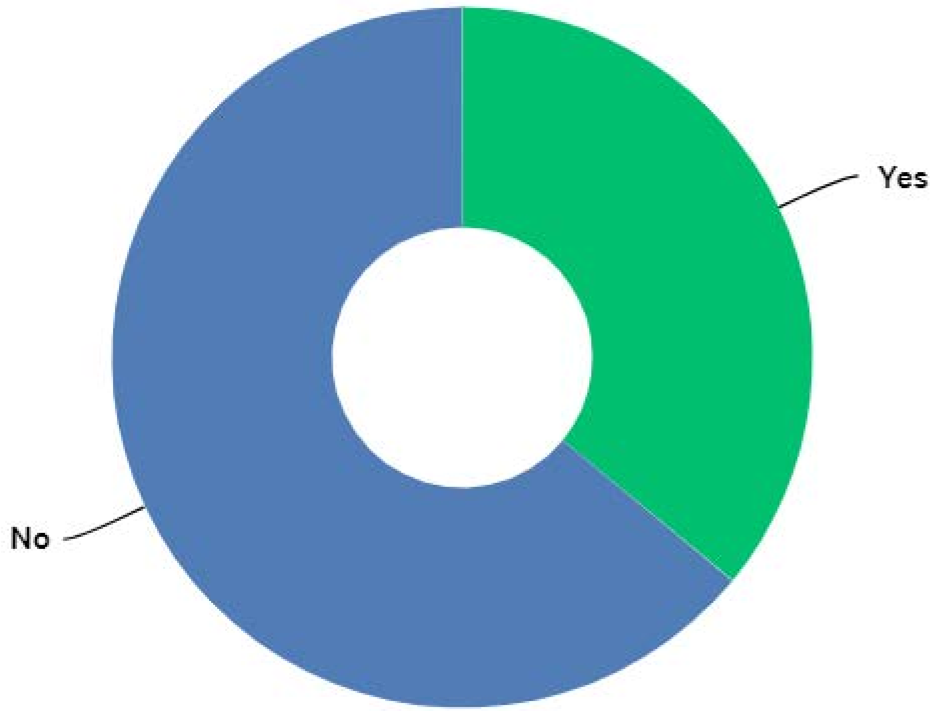
CMIT 2017 Research – Surveyed 105,000 US Businesses

Has your business been compromised by ransomware, a cryptovirus or other infection in the last 12 months?



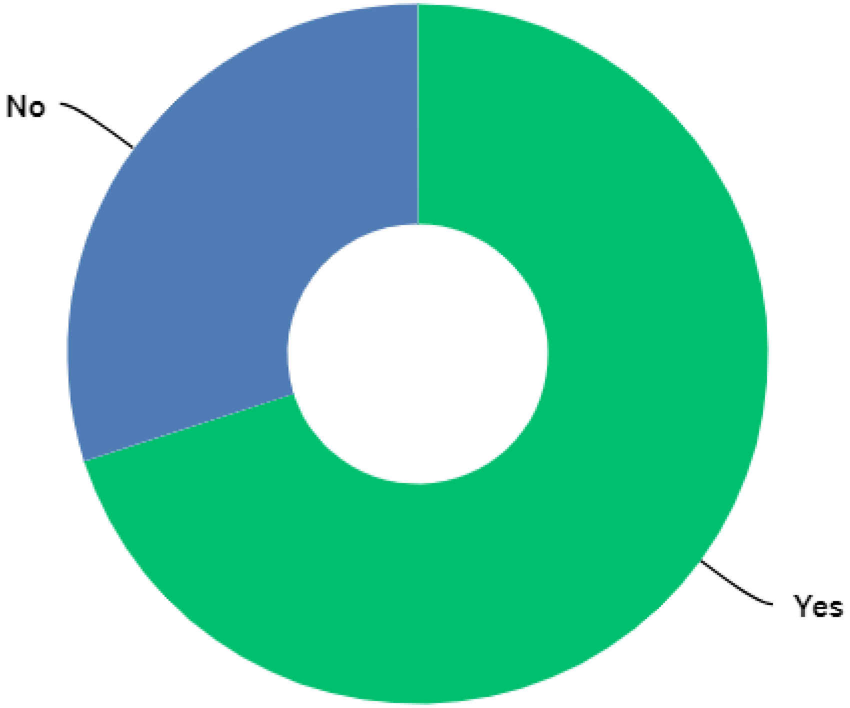
CMIT 2017 Research – Surveyed 105,000 US Businesses

Do you know a business that has been compromised?



CMIT 2017 Research – Surveyed 105,000 US Businesses

Are you willing to pay for cyber-threat protection?



IBM Security

United States

Average costs

Average Cost of a Data Breach

$7.91

Million Dollars

Average Cost Per Record

$233

Dollars

Average times

Average time to identify a breach

201 Days

Average time to contain a breach

52 Days

Top 3 cost reducing factors

1. Incident response team
2. Extensive use of encryption
3. Employee training

Top 3 cost increasing factors

1. Compliance failures
2. Third party involvement
3. Extensive cloud migration

Ponemon INSTITUTE

RISK to SMB is BIG… Very BIG

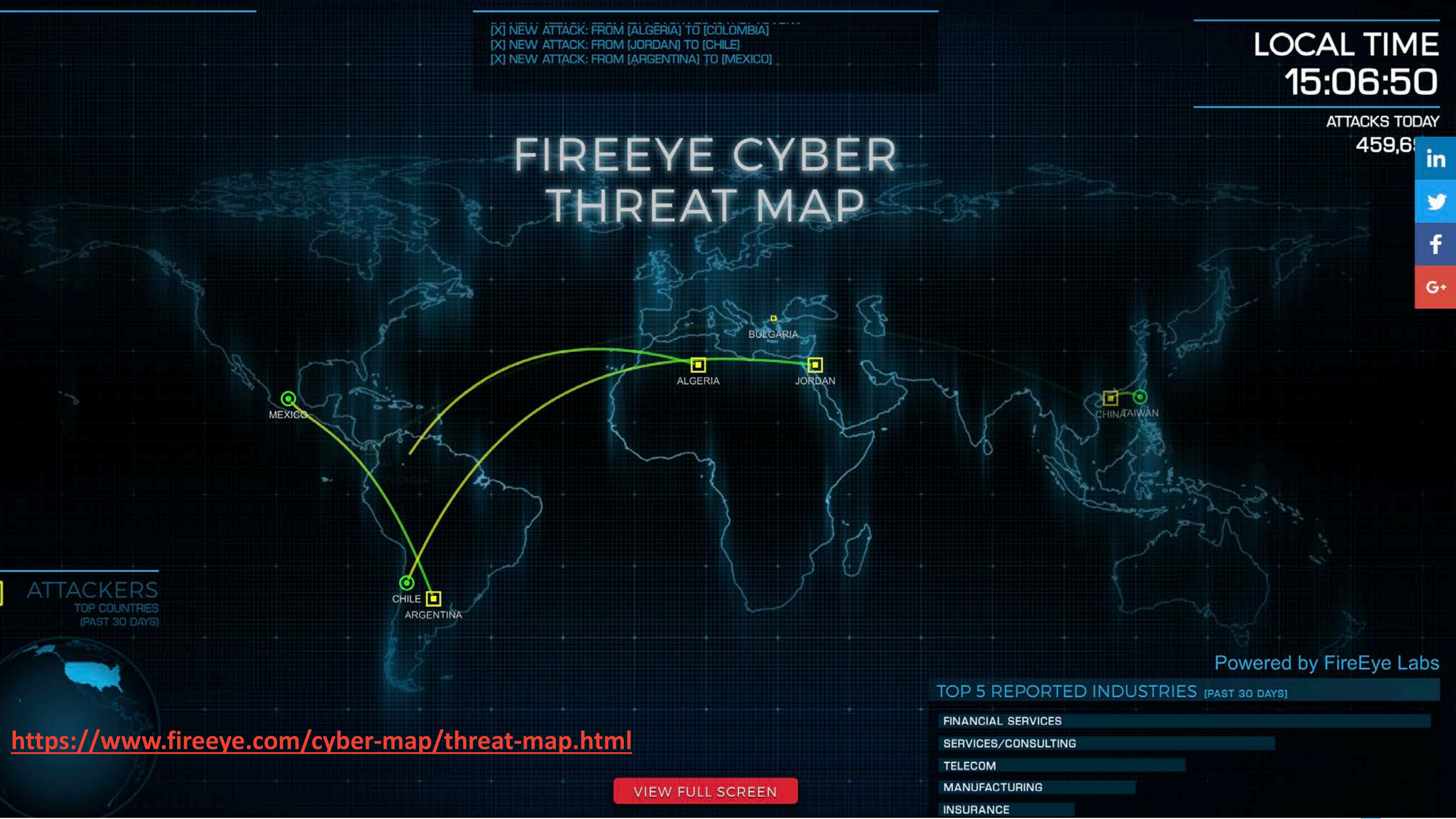
According to the Verizon Data Breach Investigation Report:

- 61% of breaches occurred in smaller businesses last year
- Increase from the previous year's 53%

According to UPS Capital:

- Breaches cost small businesses between $84,000 and $148,000
- 33% of firms required 3+ days to recover
- 60% of small businesses go out of business within six months of a breach

60-80% of attacks target small merchants (Source: PCI Council)



[X] NEW ATTACK: FROM [ALGERIA] TO [COLOMBIA]
[X] NEW ATTACK: FROM [JORDAN] TO [CHILE]
[X] NEW ATTACK: FROM [ARGENTINA] TO [MEXICO]

FIREEYE CYBER THREAT MAP

LOCAL TIME
15:06:50

ATTACKS TODAY
459,6

ATTACKERS
TOP COUNTRIES
(PAST 30 DAYS)

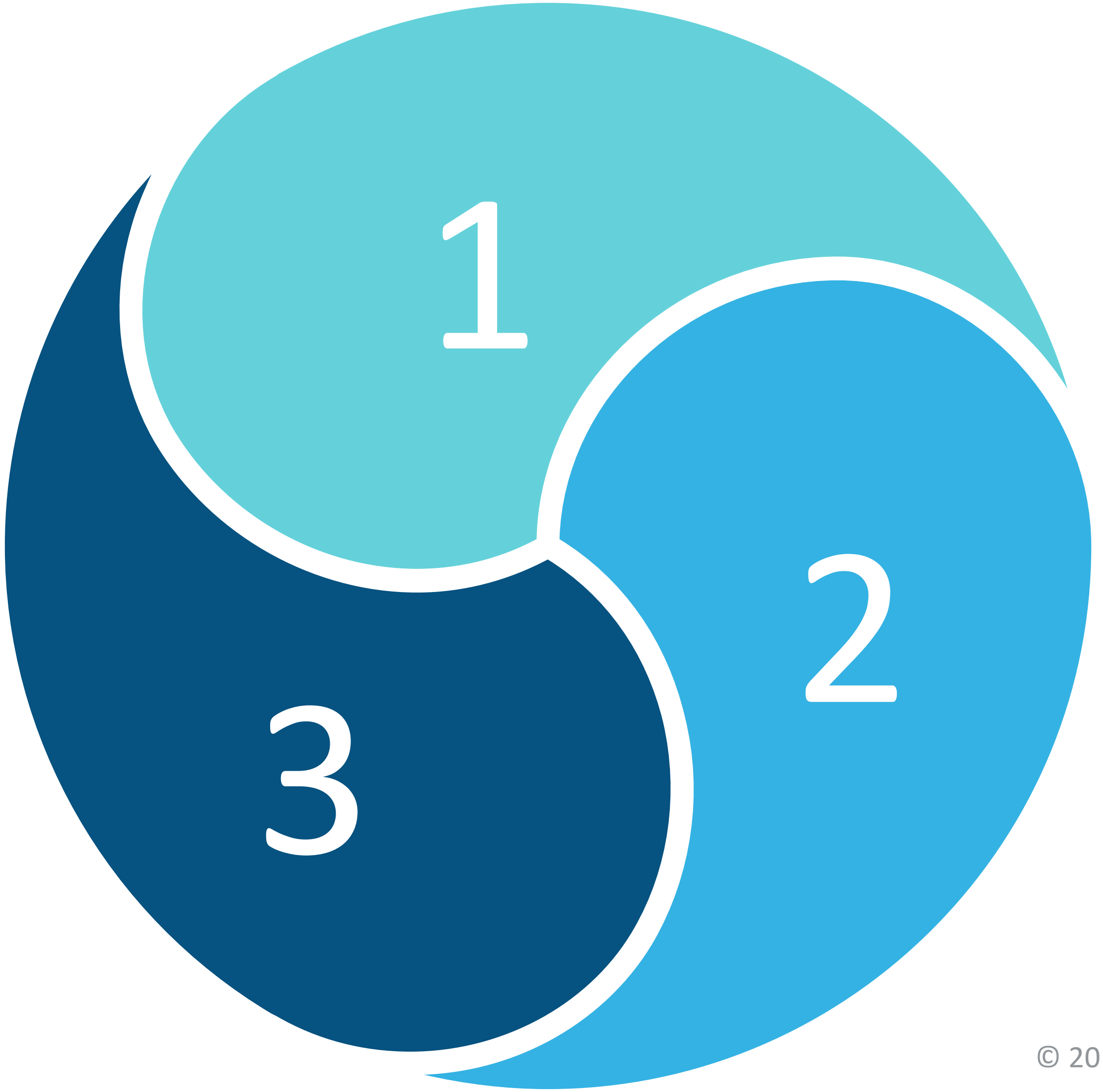
Powered by FireEye Labs

TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)

- FINANCIAL SERVICES
- SERVICES/CONSULTING
- TELECOM
- MANUFACTURING
- INSURANCE

https://www.fireeye.com/cyber-map/threat-map.html

The Perfect Storm



1 CYBER ATTACK ECONOMY

POWERED BY BITCOIN
RARELY REPORTED OR PROSECUTED
THE WILD, WILD, WEST

2 THREAT ECOSYSTEM

NEW SOFTWARE INDUSTRY
RANSOMWARE AS A SERVICE

3 RICH TARGETS

28 MILLION SMALL BUSINESS IN USA
EASIER TARGETS BEYOND FORTUNE 500

How much money is in the world?

$80 trillion

According to the CIA

Source: Business Insider November, 2017

Economists estimate that only

8%

of the world's currency exists
as physical cash.

The Malware Economy

Estimated to be a multi-billion dollar business

- Exploit kits are being sold or rented like commercial products
- No expertise required

Rate of profit-to-effort is 20-to-1

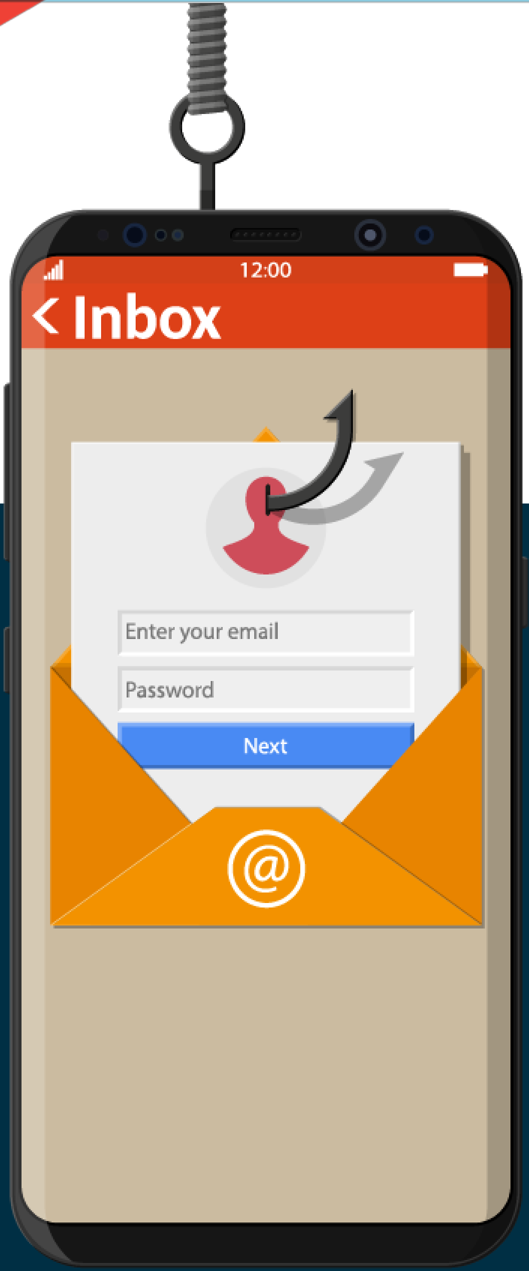
The New Face of Organized Crime

Hackers are no longer lone wolves. They're now banding together to run fewer—yet much larger—attacks, similar to the traditional crime rings of the 20th century.

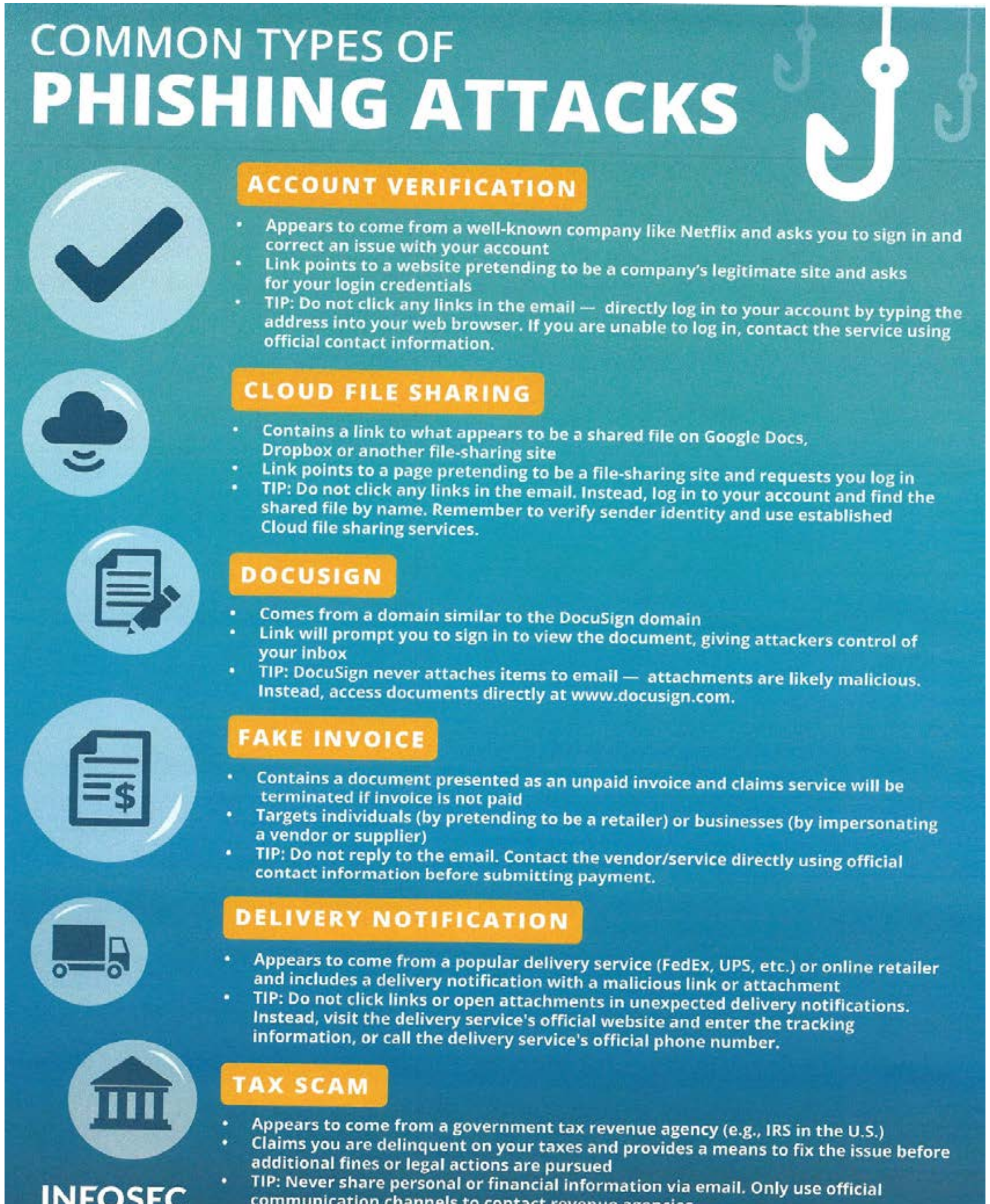
80% of cyber-attacks are driven by **organized crime rings**, in which data, tools, and expertise are widely shared.[1]

Phishing Statistics

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication.



- 43% of targeted spear phishing attacks were directed to business with 250 or fewer employees. (Symantec ITSR 2018)
- 23% of phishing emails are opened by recipients. (Verizon DBIR)
- 11% of individuals that open a phishing email also click on the link or attachment in the message. (Verizon DBIR)



COMMON TYPES OF PHISHING ATTACKS

ACCOUNT VERIFICATION

- Appears to come from a well-known company like Netflix and asks you to sign in and correct an issue with your account
- Link points to a website pretending to be a company's legitimate site and asks for your login credentials
- TIP: Do not click any links in the email — directly log in to your account by typing the address into your web browser. If you are unable to log in, contact the service using official contact information.

CLOUD FILE SHARING

- Contains a link to what appears to be a shared file on Google Docs, Dropbox or another file-sharing site
- Link points to a page pretending to be a file-sharing site and requests you log in
- TIP: Do not click any links in the email. Instead, log in to your account and find the shared file by name. Remember to verify sender identity and use established Cloud file sharing services.

DOCUSIGN

- Comes from a domain similar to the DocuSign domain
- Link will prompt you to sign in to view the document, giving attackers control of your inbox
- TIP: DocuSign never attaches items to email — attachments are likely malicious. Instead, access documents directly at www.docusign.com.

FAKE INVOICE

- Contains a document presented as an unpaid invoice and claims service will be terminated if invoice is not paid
- Targets individuals (by pretending to be a retailer) or businesses (by impersonating a vendor or supplier)
- TIP: Do not reply to the email. Contact the vendor/service directly using official contact information before submitting payment.

DELIVERY NOTIFICATION

- Appears to come from a popular delivery service (FedEx, UPS, etc.) or online retailer and includes a delivery notification with a malicious link or attachment
- TIP: Do not click links or open attachments in unexpected delivery notifications. Instead, visit the delivery service's official website and enter the tracking information, or call the delivery service's official phone number.

TAX SCAM

- Appears to come from a government tax revenue agency (e.g., IRS in the U.S.)
- Claims you are delinquent on your taxes and provides a means to fix the issue before additional fines or legal actions are pursued
- TIP: Never share personal or financial information via email. Only use official communication channels to contact revenue agencies

INFOSEC

3

Opportunities

Due Diligence

01

After Closing

02

Operations

03

MAIN STREET Cybersecurity Act of 2017

IDENTIFY ASSETS

PROTECT DATA

DETECT PROBLEMS

RESPOND QUICKLY

RECOVER BUSINESS

Passed August 14, 2018 into US law.

Click for the full text of the law.

Due

Diligence

Due Diligence

01

If you are the buyer : is the target safe?

1. Have they experienced a ransomware, malware or phishing attempt?
2. Is the company network secure?
3. Is a hacker hiding within the systems?
4. Have they experienced a data breach?

If you are the seller : do you have unmitigated liabilities?

1. Do you have security policies and procedures?
2. Do you have multi-layered cyber defenses?
3. When was your last cybersecurity assessment?
4. Do you have security information and event management?
5. Who is responsible for cyber security?

Step 1 : Where are you?

- IDENTIFY ASSETS
- PROTECT DATA
- DETECT PROBLEMS
- RESPOND QUICKLY
- RECOVER BUSINESS

Industry Standards and Best Practices to help organizations manage cybersecurity risks.
Version 1.0, February 12, 2014

Perform Cybersecurity Assessment. Evaluate GAPS

IDENTIFY ASSETS

PROTECT DATA

DETECT PROBLEMS

RESPOND QUICKLY

RECOVER BUSINESS

Industry Standards and Best Practices to help organizations manage cybersecurity risks.
Version 1.0, February 12, 2014

Inspect Supply Chain.

IDENTIFY ASSETS

PROTECT DATA

DETECT PROBLEMS

RESPOND QUICKLY

RECOVER BUSINESS

Industry Standards and Best Practices to help organizations manage cybersecurity risks.

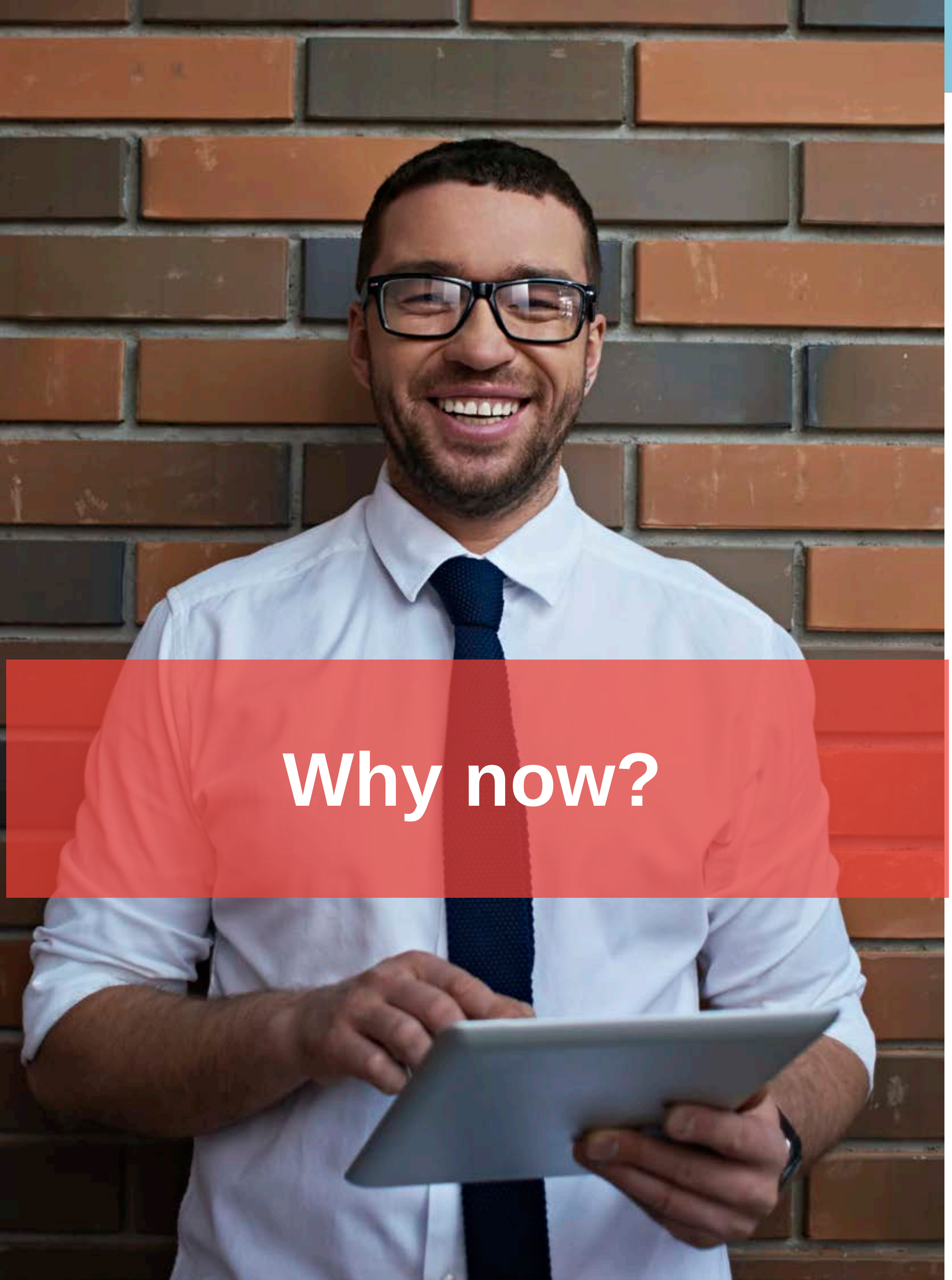
Version 1.0, February 12, 2014

After

Closing

After
Closing

02



Why now?

STRENGTHEN YOUR DEFENSES

Verify crown jewels

Run the data backups and RESTORE. Prove the process, people, and technology operate as you require.

Make security an executive level responsibility

Correct exposures found in due diligence.
Strengthen your supply chain security.
Create an informed security culture within the organization.

After Closing

First 90 Days

Verify.

1. Verify Crown Jewels Backup and Restore.
2. Name Your Security Executive.
3. Assign budget.

Second 90 days

Protect.

1. Security QBR.
2. Improve defenses.
3. Invest in staff training.

Next 6 months

Improve.

1. Execute specific projects.
2. Institutionalize procedures.
3. Track key metrics.

Operations

Operations

03

Operations

EXECUTIVE LEADERSHIP

MULTI-LAYERED TECHNICAL DEFENSES

REGULAR REPORTING

POLICIES & PROCEDURES

PERIODIC TESTS

STAFF TRAINING

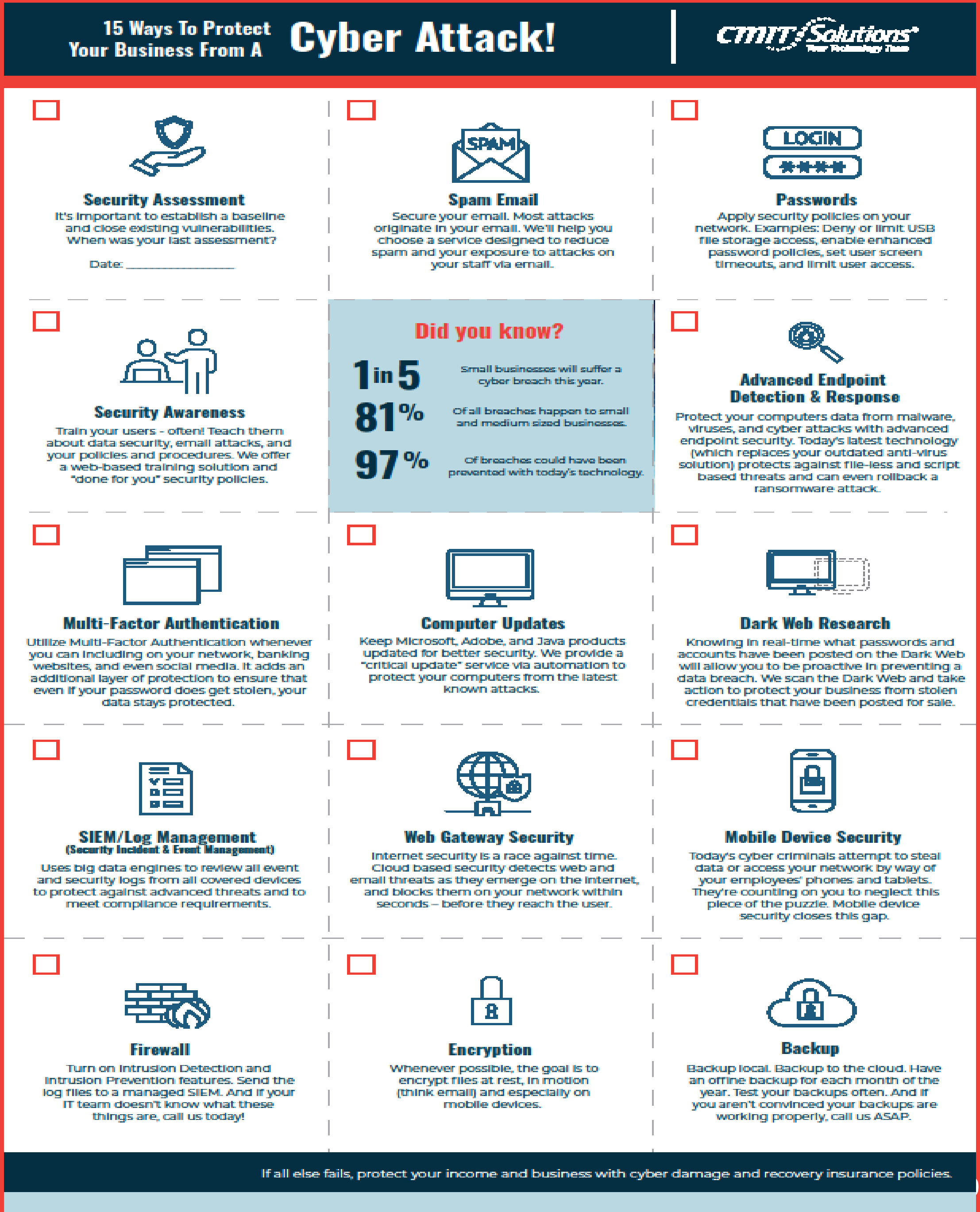
Grab your

DIY Cyber Protection Kit.

Cyber attacks can happen to anyone.

No business is too small.

16 actions that can be taken to secure your business



15 Ways To Protect Your Business From A Cyber Attack!

CMIT Solutions® Your Technology Team

□ **Security Assessment**
It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date: ________________

□ **Spam Email**
Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

□ **Passwords**
Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

□ **Security Awareness**
Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

Did you know?

1 in 5 — Small businesses will suffer a cyber breach this year.

81% — Of all breaches happen to small and medium sized businesses.

97% — Of breaches could have been prevented with today's technology.

□ **Advanced Endpoint Detection & Response**
Protect your computers data from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script based threats and can even rollback a ransomware attack.

□ **Multi-Factor Authentication**
Utilize Multi-Factor Authentication whenever you can including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.

□ **Computer Updates**
Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.

□ **Dark Web Research**
Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.

□ **SIEM/Log Management**
(Security Incident & Event Management)
Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.

□ **Web Gateway Security**
Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds – before they reach the user.

□ **Mobile Device Security**
Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

□ **Firewall**
Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!

□ **Encryption**
Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.

□ **Backup**
Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

If all else fails, protect your income and business with cyber damage and recovery insurance policies.

Prevention-What Can Your Business Do

Train Employees (Culture)

Education is critical as employees are the single most important aspect of security (training kits)

Explain Risks

Establish Acceptable Use Policy-Company owned devices (travel policies, mobile device policies, role/level of person, manage the person/device)

Purchase Cyber Insurance Policy

Especially Regulated Industries-Legal, Medical & Financial (how much is your horse worth?)

Be careful what you share on Social Media

Hackers love to comb social media in order to find out more about you, and exploit that information

Require Password Management & Enable Multi-Factor Authentication

Especially online banking, hosted software applications (QB online) or Business Social Media Accounts

8+ characters, frequency of change, use of stolen pwds, password managers/single sign-on, MFA/2FA, sim cards, keys, hashing/encryption/keys

Hire Professional IT Support, Outsource, or Direct Hire

Ever evolving threat landscape, pace of change with technology, 3rd party perspective

Wire Transfers

Establish approval policies (Use the phone & remember to say thank you for using the phone)

Basic Prevention - What We Do To Help Our Clients

Staff Security Training

We educate our clients & encourage them to call us when suspicious (Email Button, training kits)

Firewalls

Filtering/blocking specified inbound and outbound traffic (Firewall Management)

Anti-virus & Anti-malware

Stopping viruses and other malware (There are good options, a few dollars/month, do not use free-ware)

Patching

Ensuring computers and servers have latest patches installed (Depend on bus apps, may need testing) **(Win10, Win7)**

Encryption

Encoding a message, disk, or information in such a way that only authorized parties can access it (LinkedIn example)

Email Spam Filtering

All emails are analyzed by cloud service before hitting your server (advanced threat protection is on the market)

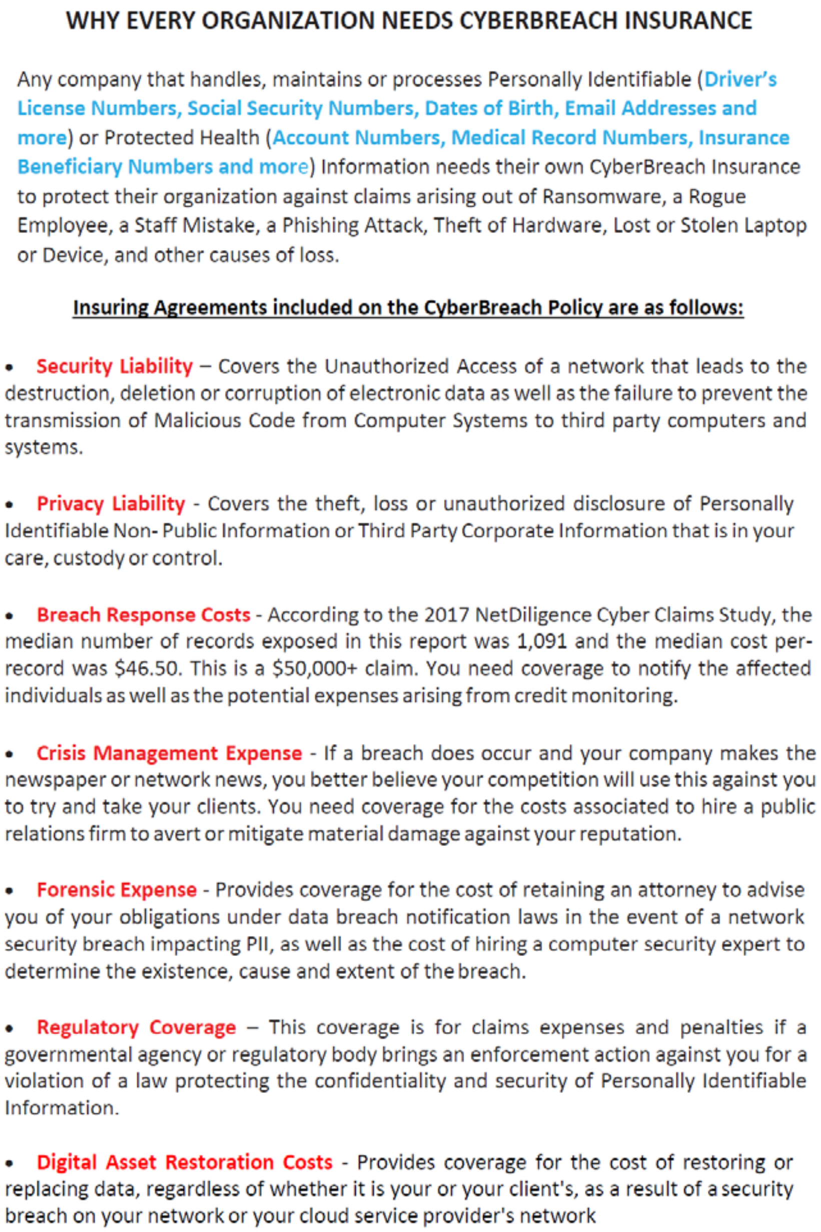
DNS Protection

Blocks dangerous and questionable websites (should be mandatory)

Backups

Data on Server is backed up every day-do not store any important data on local drives (regularly tested)

Why is Cyber Insurance Needed



WHY EVERY ORGANIZATION NEEDS CYBERBREACH INSURANCE

Any company that handles, maintains or processes Personally Identifiable (Driver's License Numbers, Social Security Numbers, Dates of Birth, Email Addresses and more) or Protected Health (Account Numbers, Medical Record Numbers, Insurance Beneficiary Numbers and more) Information needs their own CyberBreach Insurance to protect their organization against claims arising out of Ransomware, a Rogue Employee, a Staff Mistake, a Phishing Attack, Theft of Hardware, Lost or Stolen Laptop or Device, and other causes of loss.

Insuring Agreements included on the CyberBreach Policy are as follows:

- Security Liability – Covers the Unauthorized Access of a network that leads to the destruction, deletion or corruption of electronic data as well as the failure to prevent the transmission of Malicious Code from Computer Systems to third party computers and systems.

- Privacy Liability - Covers the theft, loss or unauthorized disclosure of Personally Identifiable Non- Public Information or Third Party Corporate Information that is in your care, custody or control.

- Breach Response Costs - According to the 2017 NetDiligence Cyber Claims Study, the median number of records exposed in this report was 1,091 and the median cost per-record was $46.50. This is a $50,000+ claim. You need coverage to notify the affected individuals as well as the potential expenses arising from credit monitoring.

- Crisis Management Expense - If a breach does occur and your company makes the newspaper or network news, you better believe your competition will use this against you to try and take your clients. You need coverage for the costs associated to hire a public relations firm to avert or mitigate material damage against your reputation.

- Forensic Expense - Provides coverage for the cost of retaining an attorney to advise you of your obligations under data breach notification laws in the event of a network security breach impacting PII, as well as the cost of hiring a computer security expert to determine the existence, cause and extent of the breach.

- Regulatory Coverage – This coverage is for claims expenses and penalties if a governmental agency or regulatory body brings an enforcement action against you for a violation of a law protecting the confidentiality and security of Personally Identifiable Information.

- Digital Asset Restoration Costs - Provides coverage for the cost of restoring or replacing data, regardless of whether it is your or your client's, as a result of a security breach on your network or your cloud service provider's network

- **Business Income Coverage** - If your business is unable to operate due to a cyber breach of your network or the network of your cloud service provider, this coverage provides business interruption coverage.

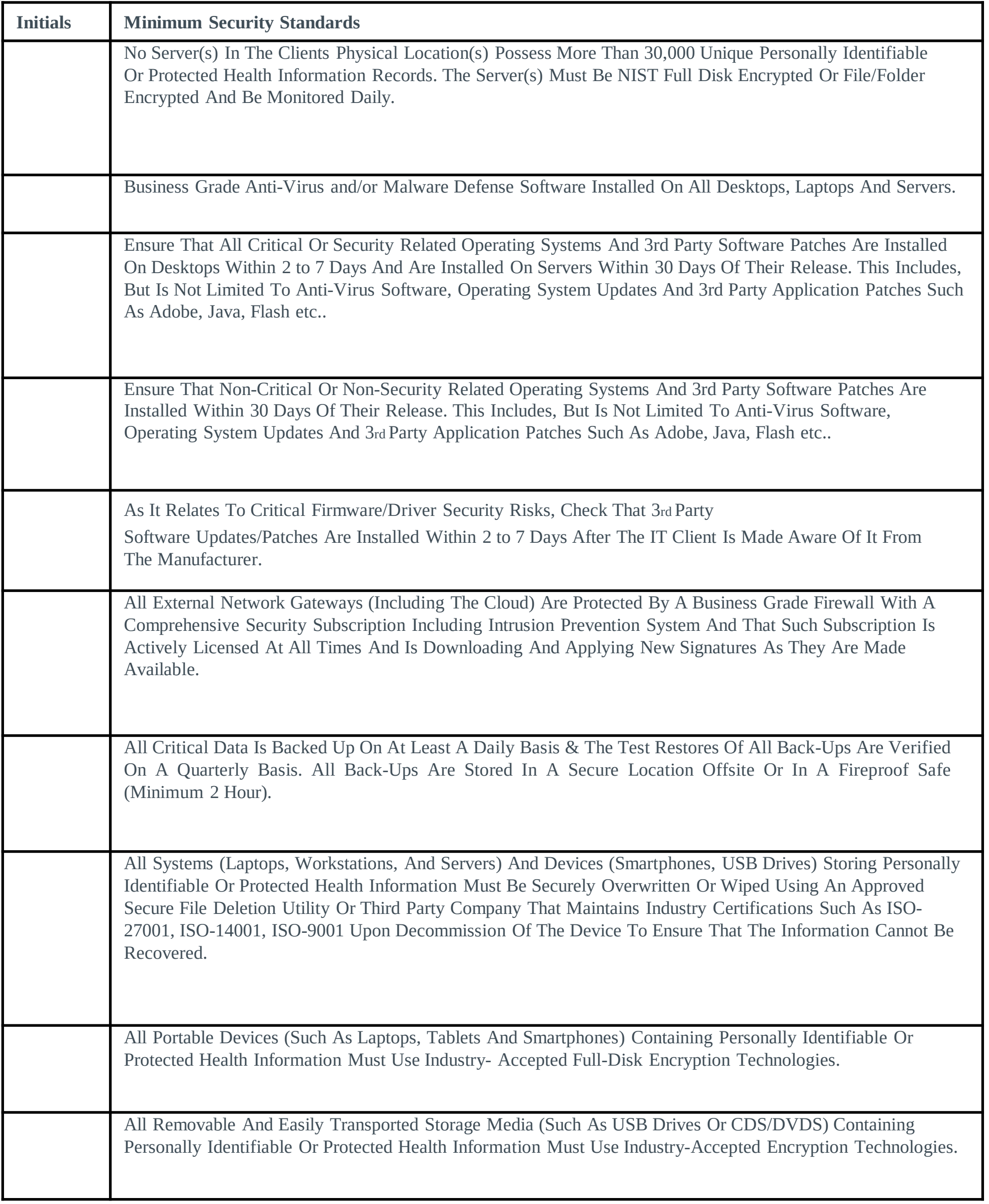
- **Cyber Extortion Threat** – Cyber extortionists may threaten to harm you, your reputation, or your property if you do not comply with their demands. Cyber extortion can take many forms. For example, the cybercriminal may use "ransomware" to encrypt your data, which means you can't read your data without the encryption key – and the cybercriminal will withhold this key until payment is made. This coverage is needed for situations where you must make a payment to eliminate credible threats.

- **Cyber-Theft Loss** – Cyber-attacks are now more sophisticated than ever before. This coverage will reimburse your company for the loss of money due to the unauthorized transfer of funds, service credits or tangible property.

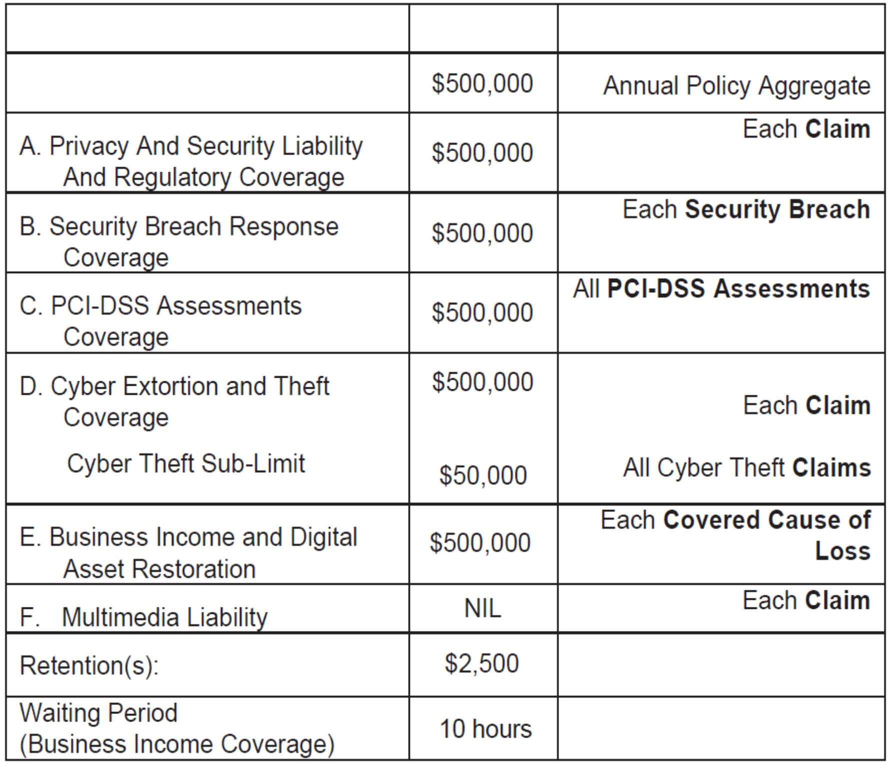
- **Cyber-Fraud Event** – This occurs when a criminal enterprise disguises themselves as an employee, client or vendor and tricks someone at your organization into transferring funds to an account under their control. This could come from a phishing attack or social engineering email, text or instant message.

- **PCI DSS Assessment Coverage** – Did you know that businesses are required to implement a set of security standards to protect credit card data? This insuring agreement provides coverage for assessments, fines or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.

Sample Cyber Insurance Requirements and Coverage



Initials	Minimum Security Standards
	No Server(s) In The Clients Physical Location(s) Possess More Than 30,000 Unique Personally Identifiable Or Protected Health Information Records. The Server(s) Must Be NIST Full Disk Encrypted Or File/Folder Encrypted And Be Monitored Daily.
	Business Grade Anti-Virus and/or Malware Defense Software Installed On All Desktops, Laptops And Servers.
	Ensure That All Critical Or Security Related Operating Systems And 3rd Party Software Patches Are Installed On Desktops Within 2 to 7 Days And Are Installed On Servers Within 30 Days Of Their Release. This Includes, But Is Not Limited To Anti-Virus Software, Operating System Updates And 3rd Party Application Patches Such As Adobe, Java, Flash etc..
	Ensure That Non-Critical Or Non-Security Related Operating Systems And 3rd Party Software Patches Are Installed Within 30 Days Of Their Release. This Includes, But Is Not Limited To Anti-Virus Software, Operating System Updates And 3rd Party Application Patches Such As Adobe, Java, Flash etc..
	As It Relates To Critical Firmware/Driver Security Risks, Check That 3rd Party Software Updates/Patches Are Installed Within 2 to 7 Days After The IT Client Is Made Aware Of It From The Manufacturer.
	All External Network Gateways (Including The Cloud) Are Protected By A Business Grade Firewall With A Comprehensive Security Subscription Including Intrusion Prevention System And That Such Subscription Is Actively Licensed At All Times And Is Downloading And Applying New Signatures As They Are Made Available.
	All Critical Data Is Backed Up On At Least A Daily Basis & The Test Restores Of All Back-Ups Are Verified On A Quarterly Basis. All Back-Ups Are Stored In A Secure Location Offsite Or In A Fireproof Safe (Minimum 2 Hour).
	All Systems (Laptops, Workstations, And Servers) And Devices (Smartphones, USB Drives) Storing Personally Identifiable Or Protected Health Information Must Be Securely Overwritten Or Wiped Using An Approved Secure File Deletion Utility Or Third Party Company That Maintains Industry Certifications Such As ISO-27001, ISO-14001, ISO-9001 Upon Decommission Of The Device To Ensure That The Information Cannot Be Recovered.
	All Portable Devices (Such As Laptops, Tablets And Smartphones) Containing Personally Identifiable Or Protected Health Information Must Use Industry- Accepted Full-Disk Encryption Technologies.
	All Removable And Easily Transported Storage Media (Such As USB Drives Or CDS/DVDS) Containing Personally Identifiable Or Protected Health Information Must Use Industry-Accepted Encryption Technologies.



	$500,000	Annual Policy Aggregate
A. Privacy And Security Liability And Regulatory Coverage	$500,000	Each **Claim**
B. Security Breach Response Coverage	$500,000	Each **Security Breach**
C. PCI-DSS Assessments Coverage	$500,000	All **PCI-DSS Assessments**
D. Cyber Extortion and Theft Coverage Cyber Theft Sub-Limit	$500,000 $50,000	Each **Claim** All Cyber Theft **Claims**
E. Business Income and Digital Asset Restoration	$500,000	Each **Covered Cause of Loss**
F. Multimedia Liability	NIL	Each **Claim**
Retention(s):	$2,500	
Waiting Period (Business Income Coverage)	10 hours	

Example Cyber Insurance Questions

Do you currently have Cyber Coverage? **YES** **NO**

Have you ever had a Cyber Claim? * **YES** **NO**

* any expense, loss or liability incurred arising from the theft, loss or unauthorized disclosure of personally identifiable information data or the unauthorized access or use of your IT network whether insured under an existing/previous insurance policy or uninsured.

Do you store:

1) Records containing non-public personal information or protected health information for more than 250,000 individuals (employees, vendors, customers, patients, etc.)? **YES** **NO**

2) More than 250,000 credit/debit cards transactions annually (PCI DSS Levels 1,2, or 3 merchant)? **YES** **NO**

Do you engage in any of the following activities? **YES** **NO**

Financial institution, hospital, sexual health clinic, substance abuse clinic, mental health clinic, hotel, tele- marketing specialist, gambling, university, professional sports club, social media business, political organization or trade union, public body, aerospace or defense, information technology, telecommunica- tions, data aggregation, Production or digital distribution of adult media content, Growing, marketing or distribution of cannabis products, Cryptocurrency (Bitcoin, etc.) transactions, investments, account management, mining or wallet service escrow services, title insurance and title services, real estate agents & brokers.

Funds Transfer Controls

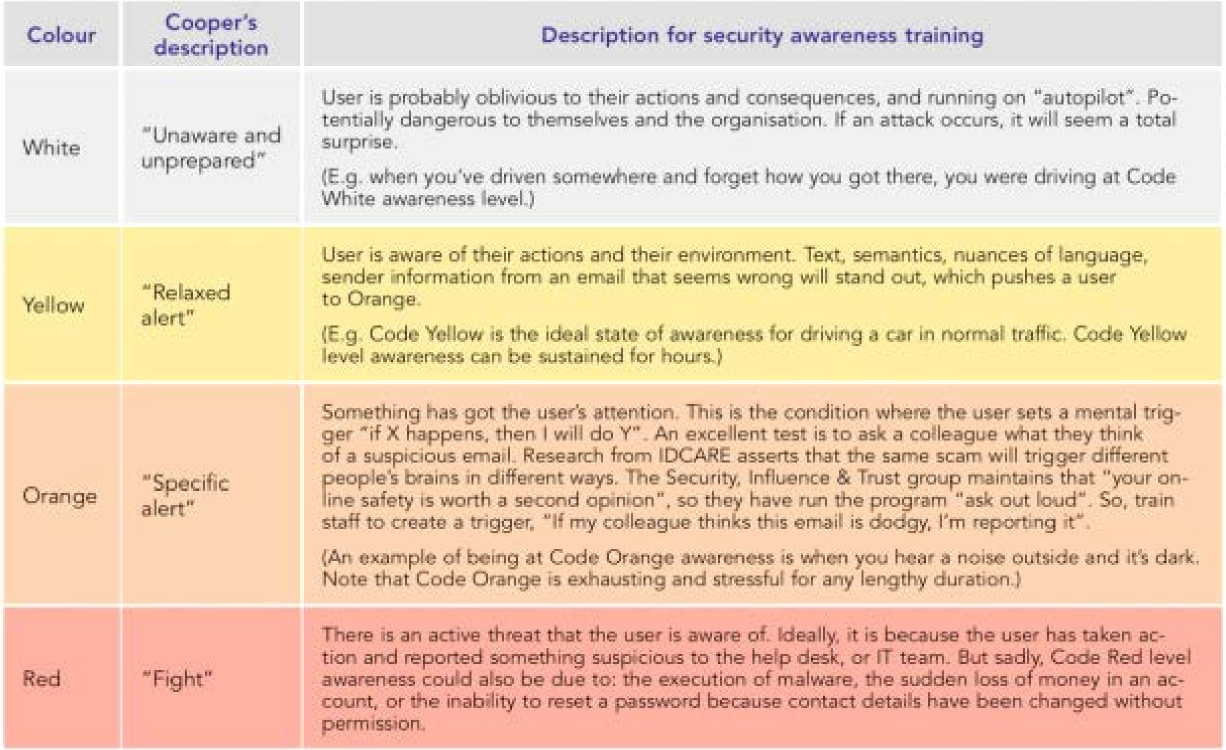
1) Are the identities of customers and vendors, as well as any new or changed contact or bank account details, agreed in writing, and confirmed by phone prior to the issuance of any funds transfers?

2) Do you require dual authorization for funds transfers greater than $5,000?

Culture of Security

The Human Firewall – Culture, Policy, & Compliance

Research presented by the University of Otago in 2016 showed that when employees fell for a **phishing attack**, they were usually away from their desk, using mobile devices that didn't necessarily display the email in full. It usually happened outside business hours, too, either late at night when they were tired, or first thing in the morning when they were busy starting their household's daily routine.



Colour	Cooper's description	Description for security awareness training
White	"Unaware and unprepared"	User is probably oblivious to their actions and consequences, and running on "autopilot". Potentially dangerous to themselves and the organisation. If an attack occurs, it will seem a total surprise. (E.g. when you've driven somewhere and forget how you got there, you were driving at Code White awareness level.)
Yellow	"Relaxed alert"	User is aware of their actions and their environment. Text, semantics, nuances of language, sender information from an email that seems wrong will stand out, which pushes a user to Orange. (E.g. Code Yellow is the ideal state of awareness for driving a car in normal traffic. Code Yellow level awareness can be sustained for hours.)
Orange	"Specific alert"	Something has got the user's attention. This is the condition where the user sets a mental trigger "if X happens, then I will do Y". An excellent test is to ask a colleague what they think of a suspicious email. Research from IDCARE asserts that the same scam will trigger different people's brains in different ways. The Security, Influence & Trust group maintains that "your online safety is worth a second opinion", so they have run the program "ask out loud". So, train staff to create a trigger, "If my colleague thinks this email is dodgy, I'm reporting it". (An example of being at Code Orange awareness is when you hear a noise outside and it's dark. Note that Code Orange is exhausting and stressful for any lengthy duration.)
Red	"Fight"	There is an active threat that the user is aware of. Ideally, it is because the user has taken action and reported something suspicious to the help desk, or IT team. But sadly, Code Red level awareness could also be due to: the execution of malware, the sudden loss of money in an account, or the inability to reset a password because contact details have been changed without permission.

Make security training a core part of the organizational change process by firstly training staff in personal e-safety. Topics include the privacy issues in using Facebook and communications platforms like WhatsApp, safe internet banking, and how to talk to their kids and teenagers about internet safety and cyberbullying.

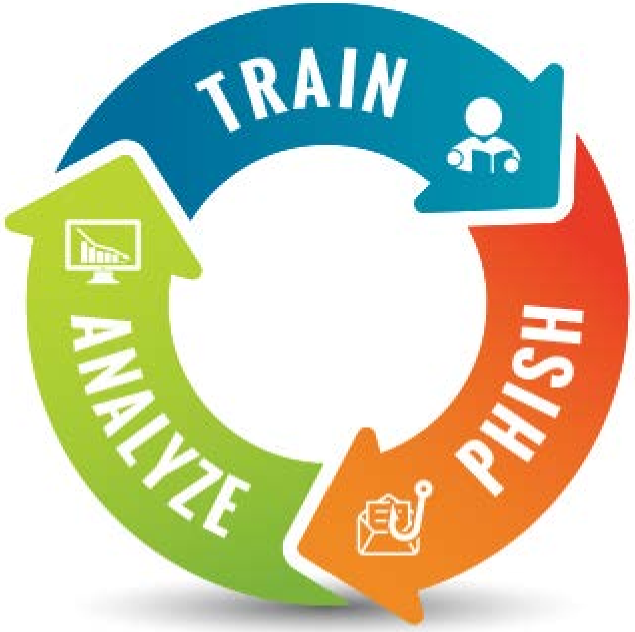
"The company is going, 'We actually give a damn about you as a human being. This stuff is important. As much as we need you to change your behaviour here at work, we're recognizing that we actually need you, as one of our valued staff, to be safe at home.'"

How companies look at a potential threat (attacks and human-error leaks) needs to change, according to security expert and CTO of RedSeal Networks, Dr. Mike Lloyd. He says companies need to stop thinking of defence as a large bank vault with a big door. Instead, they need to consider their company as a big city with many different entry and exit points and multiple areas that could contribute to a breach

THE HUMAN FIREWALL

Security Awareness Training

- Improve Security Behaviors
- Simulated Phishing attacks



Did you know the FBI estimates 80% of cyber crime starts with human error? (80% of all IT Disasters are caused by human error)

Defeating ransomware is a balance between training and technology.

Prevention

is **10% of the cost of** remediation

- 2017 study by Ponemon Institute estimates the Cost per Compromised Record averages $221 (range of $86-$402, depending on industry)

- Training costs can be as low as $6 per employee per month

Potential levels of proactive security solutions & services

Basic Security – Mandatory/Minimum Security Level	
Email Security Services	**Encryption, Archiving, Sandbox**
Web Content Filtering	**DNS**
User/End Point Device Security	Antivirus, Anti-Malware
Firewall Management	**NextGen** & UTM

Advanced Security – Security as a Strategy

2FA / SSO / PW MGMT	ID Access & Authentication
File & Disk **Encryption**	All Devices
Cybersecurity Assessment	Annual
Intrusion Detection System (IDS) – Internal Network	Monitoring of internal network
Threat Intelligence Platform (TIP) – Managed data sources.	3^{RD} Party, Gov't, Log Files, Tech. Platform
Managed **SOC** – Real-time monitoring and services	MSSP and/or Tech. Vendors
Security Awareness Training	Critical & High Impact

Total Security – Deeply Value Compliance

Log Collection [**SIEM**] – Security Information & Event Management	The entire network
Endpoint Detect & Response (**EDR**) – Next Generation anti-virus/malware, local firewall, data loss prevention, device encryption, and more (predictive)	Advanced Device Protection
Documentation to demonstrate **regulatory compliance** across industries	SOC 2, HIPAA, FINRA, PCI-DSS, NIST…
Total Device Coverage	Complete Network
User Behavior Analytics – meaningful anomalies based on user versus device events towards identifying potential threats	User patterns versus devices

4 Cybersecurity Pitfalls to Avoid

1. **Classify cybersecurity as an IT issue** – *Hackers focus their attacks on human rather than technical vulnerabilities*
2. **Dismiss cybersecurity as a large organization problem** – *Attacks are now targeting SMB’s.*
3. **Looking for a silver bullet to fix the problem** – *There is no single cybersecurity solution. There are layers of security needed.*
4. **Relying on static solutions to dynamic threats** – *Attackers are constantly developing new strategies and techniques.*

Steps that can be taken TODAY

- **Cyber Security Culture** – Initiate a Cyber security training program
- **Security Risk Assessment** – Inventory your data
  - Identify the information your business stores and uses
  - Where is it kept? How is it accessed?
  - Assess the Risk
- **Develop a Strategy for Recovery**
  - Incident Response Plan

Conclusion

1. Develop a CULTURE OF SECURITY

2. If you do not have a cybersecurity strategy, now is the time to start thinking about one

3. Prevention is 10% of the cost of remediation

Every day, I ask myself these questions.

How will the business protect itself?

What can I do to make sure you and your business are protected from cyber threats? How can we protect you without impeding growth and operations?

How will you know if you have been hacked?

What kind of early warning system can we provide that will enable you to detect and defend against attacks, but to also know that you've been compromised?

How will you recover?

What can we do to give you both the process and technology elements to assure speedy recovery?

How will you protect your clients?

How can we help you with your emergency communication plan? Can we provide the technical details your executive team needs to give your clients the assurances they need to continue doing business with you?