Cybersecurity Imperative: Computer Fraud, Hacking & Theft

March 31, 2020

Speaker

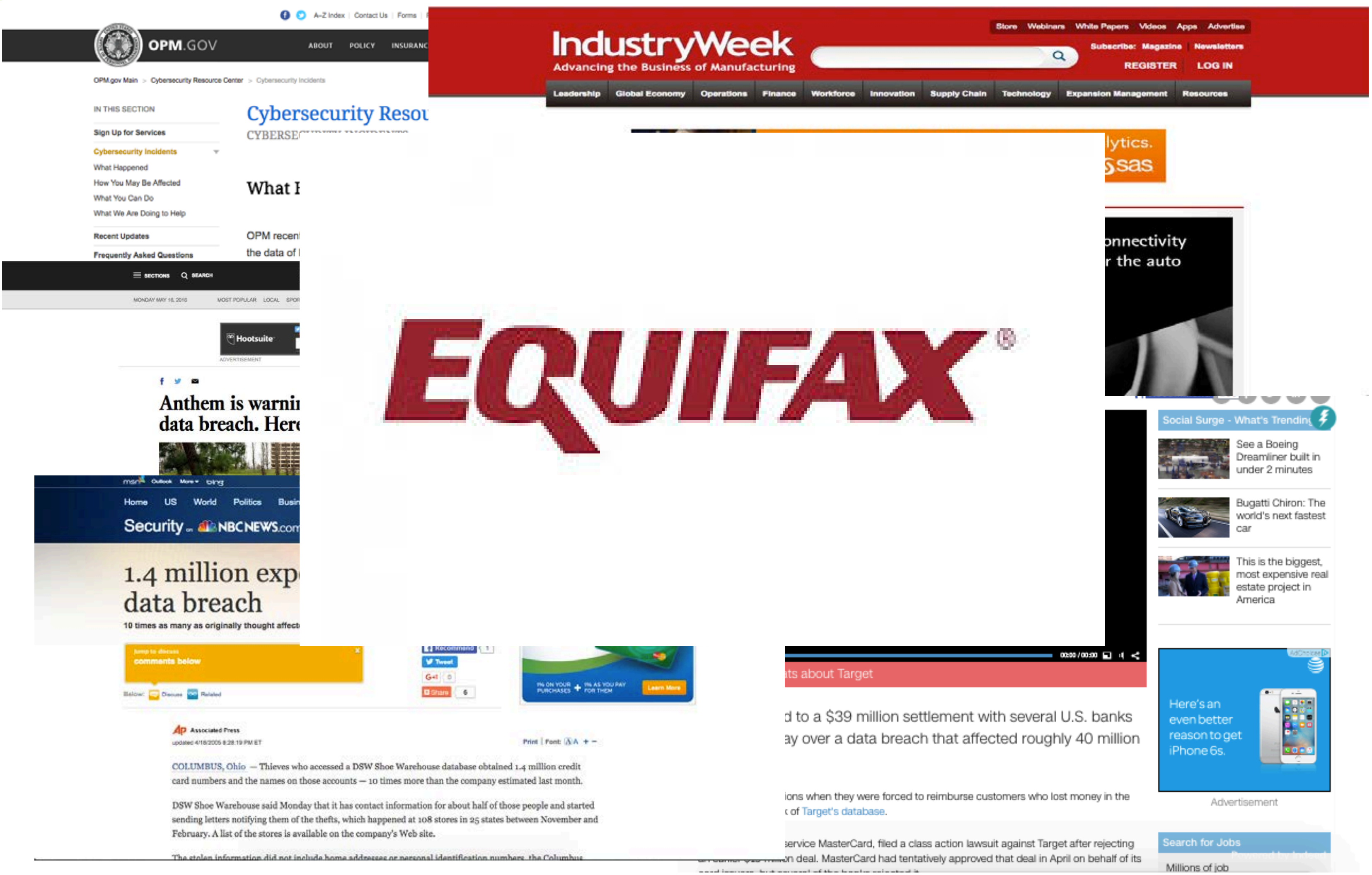
Doug Davidson
Director of Information Technology Services
(614) 947-5340
ddavidson@gbq.com

Agenda

- Current Landscape:
  - Top threats to your business
  - The cybersecurity imperative
- Protect Your Business
  - How to manage and assess risk
  - Operationalizing security
- COVID-19 Bonus Round

The Current Landscape

Cyber Issues All Over The News



A-Z Index | Contact Us | Forms

OPM.GOV ABOUT POLICY INSURANC

OPM.gov Main > Cybersecurity Resource Center > Cybersecurity Incidents

IN THIS SECTION

Sign Up for Services

Cybersecurity Incidents

What Happened

How You May Be Affected

What You Can Do

What We Are Doing to Help

Recent Updates

Frequently Asked Questions

Cybersecurity Resou

CYBERSE

What I

OPM recen

the data of

IndustryWeek

Advancing the Business of Manufacturing

Store Webinars White Papers Videos Apps Advertise

Subscribe: Magazine Newsletters

REGISTER LOG IN

Leadership Global Economy Operations Finance Workforce Innovation Supply Chain Technology Expansion Management Resources

SECTIONS SEARCH

MONDAY MAY 16, 2016 MOST POPULAR LOCAL SPOR

Anthem is warni

data breach. Here

msn Outlook More bing

Home US World Politics Busin

Security on NBCNEWS.com

1.4 million exp

data breach

10 times as many as originally thought affect

Jump to discuss comments below

Below: Discuss Related

Recommend 1 Tweet G+1 0 Share 6

Associated Press

updated 4/18/2005 8:28:19 PM ET

Print | Font: A A + −

COLUMBUS, Ohio — Thieves who accessed a DSW Shoe Warehouse database obtained 1.4 million credit card numbers and the names on those accounts — 10 times more than the company estimated last month.

DSW Shoe Warehouse said Monday that it has contact information for about half of those people and started sending letters notifying them of the thefts, which happened at 108 stores in 25 states between November and February. A list of the stores is available on the company's Web site.

The stolen information did not include home addresses or personal identification numbers, the Columbus

onnectivity

r the auto

Social Surge - What's Trending

See a Boeing Dreamliner built in under 2 minutes

Bugatti Chiron: The world's next fastest car

This is the biggest, most expensive real estate project in America

00:00 / 00:00

ts about Target

d to a $39 million settlement with several U.S. banks

ay over a data breach that affected roughly 40 million

ions when they were forced to reimburse customers who lost money in the

of Target's database.

service MasterCard, filed a class action lawsuit against Target after rejecting

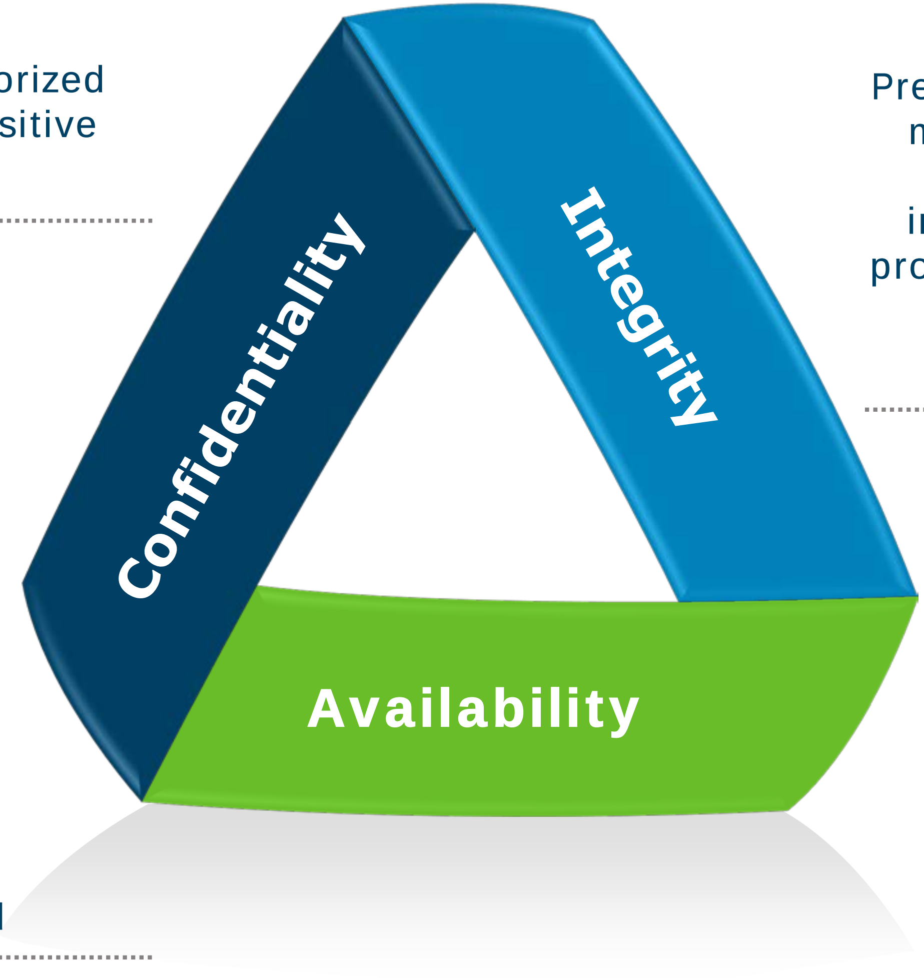
on deal. MasterCard had tentatively approved that deal in April on behalf of its

Search for Jobs

Millions of job

Information Security 101

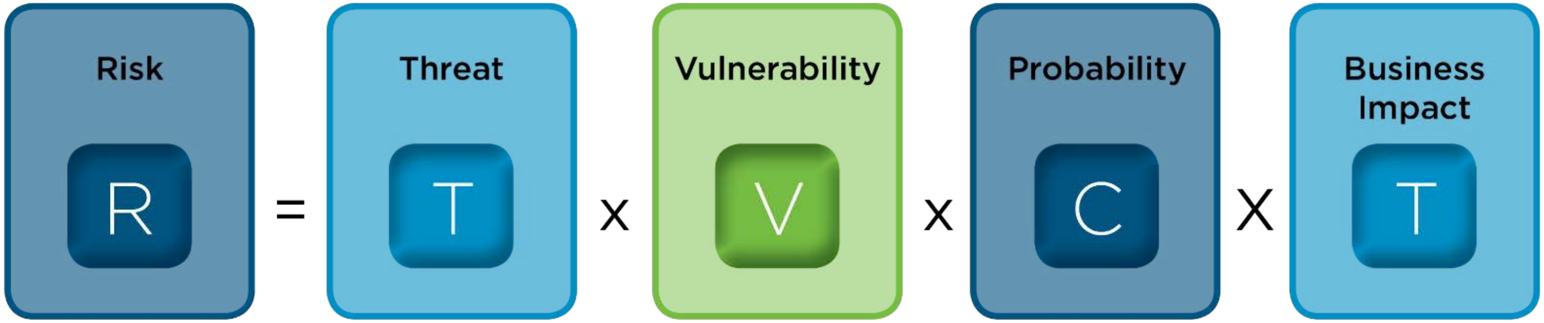
Prevents unauthorized disclosure of sensitive information



Prevents unauthorized modification of data, systems and information, thereby providing assurance of the accuracy of information

Prevents loss of access to resources and information to ensure that information is available for use when it is needed

Cyber Risk

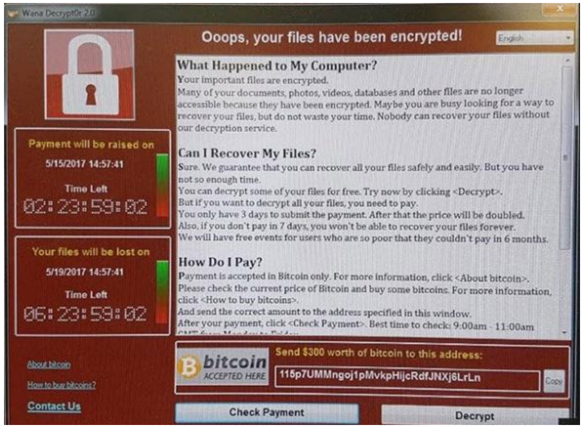


Risk R = Threat T x Vulnerability V x Probability C X Business Impact T

Cyber Risk is a function of the likelihood (probability) of an event where the bad guys (threats = hackers) will take advantage of weakness (vulnerability) to cause a loss to valued assets (business impact).

Current Cyber Threat Trends

- Why use the hard stuff when the easy stuff gets the job done?
  - Phishing
  - Business Email Compromise (BEC)
  - Account Take Over (ATO)
    - Credential Stuffing
- Malware and Evilware
  - Ransomware
  - Cryptojacking
  - Destructive malware



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on: 5/15/2017 14:57:41

Time Left: 02:23:59:02

Your files will be lost on: 5/19/2017 14:57:41

Time Left: 06:23:59:02

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

- Why beat your head against defenses when there are weak spots?
  - Pick a vulnerability – the patch race
  - 3rd parties
- Technical Exploitation and Penetration
  - Exploits
  - Zero day exploits
  - LOL – Living off the land

Threats: Who Are the Attackers?

Phishing

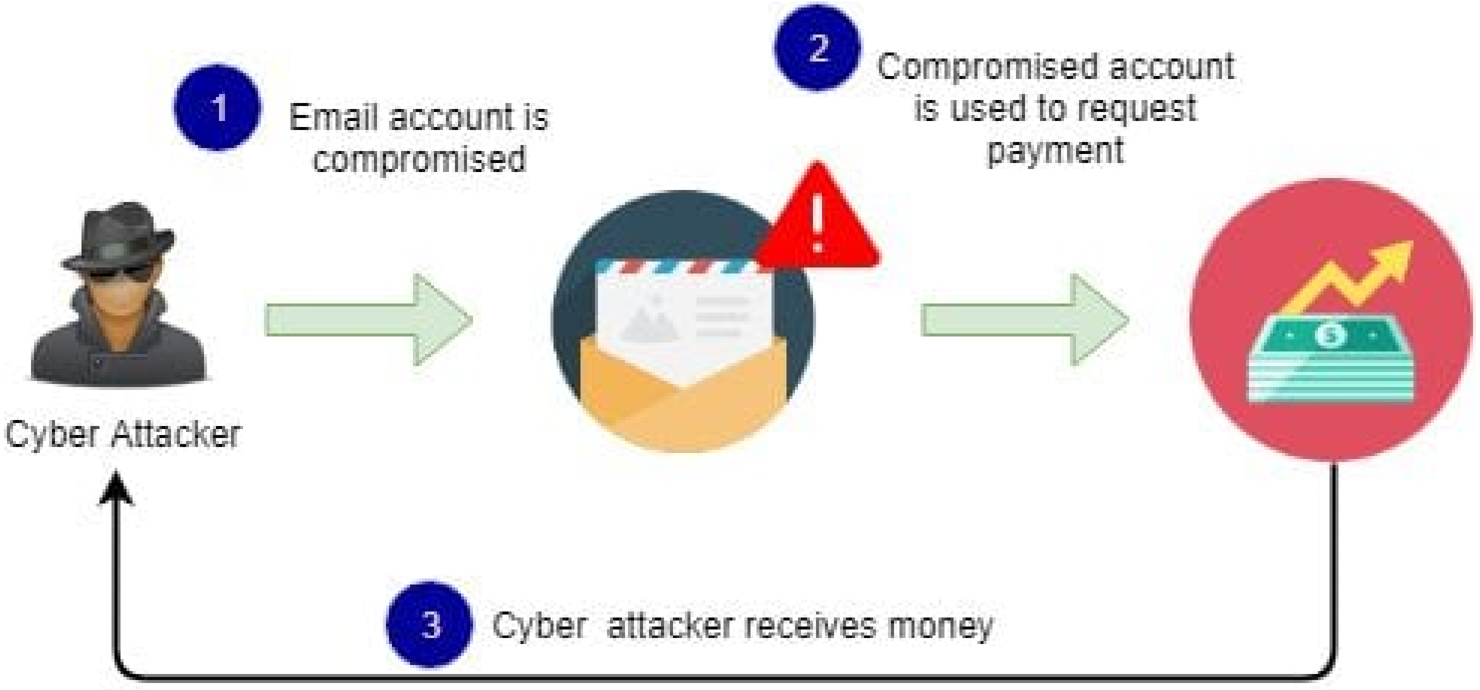
Hmm...
I smell something phishy about this!!
Click here...
to verify your bank account information.

Definition

Attempting to obtain sensitive information such as usernames, passwords and bank details (MONEY) for malicious reasons, by disguising as a trustworthy entity in an electronic source.

- Number 1 vector of attack (links and attachments)
- Not just an email – attacks on Facebook, LinkedIn and text too
- Security Awareness Campaigns
- Single biggest hacking source that you can directly impact

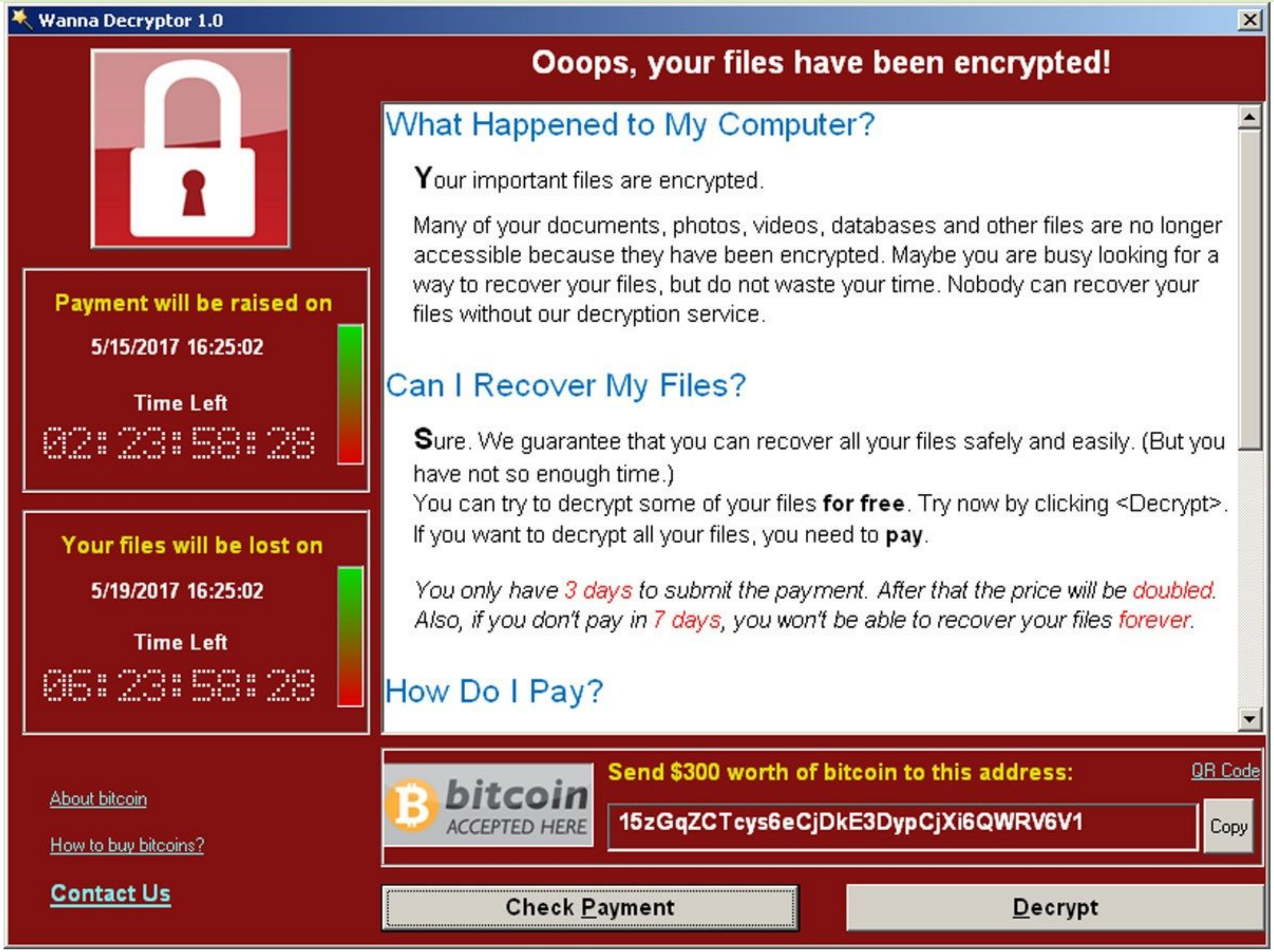
Business Email Compromise


1
Email account is compromised
2
Compromised account is used to request payment
Cyber Attacker
3
Cyber attacker receives money

Business Email Compromise - Safeguards

- **Protect the keys**
  - **Strong passwords (14+ characters, mixed with upper, lower, numbers, special characters)**
  - **Two factor authentication**
- **Train staff to detect and report suspicious behaviors**
- **Train staff not to do "dumb stuff"**
- Routinely audit email
  - Email accounts looking for old accounts
  - Email rules looking for odd rules in unexpected places
- Test your email technology stack
- **Consider cyber liability / cyber crime insurance**
- **Have an incident response plan**
  - **Who to call**
  - **What to do**

Ransomware



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 16:25:02

Time Left

02:23:58:28

Your files will be lost on

5/19/2017 16:25:02

Time Left

06:23:58:28

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

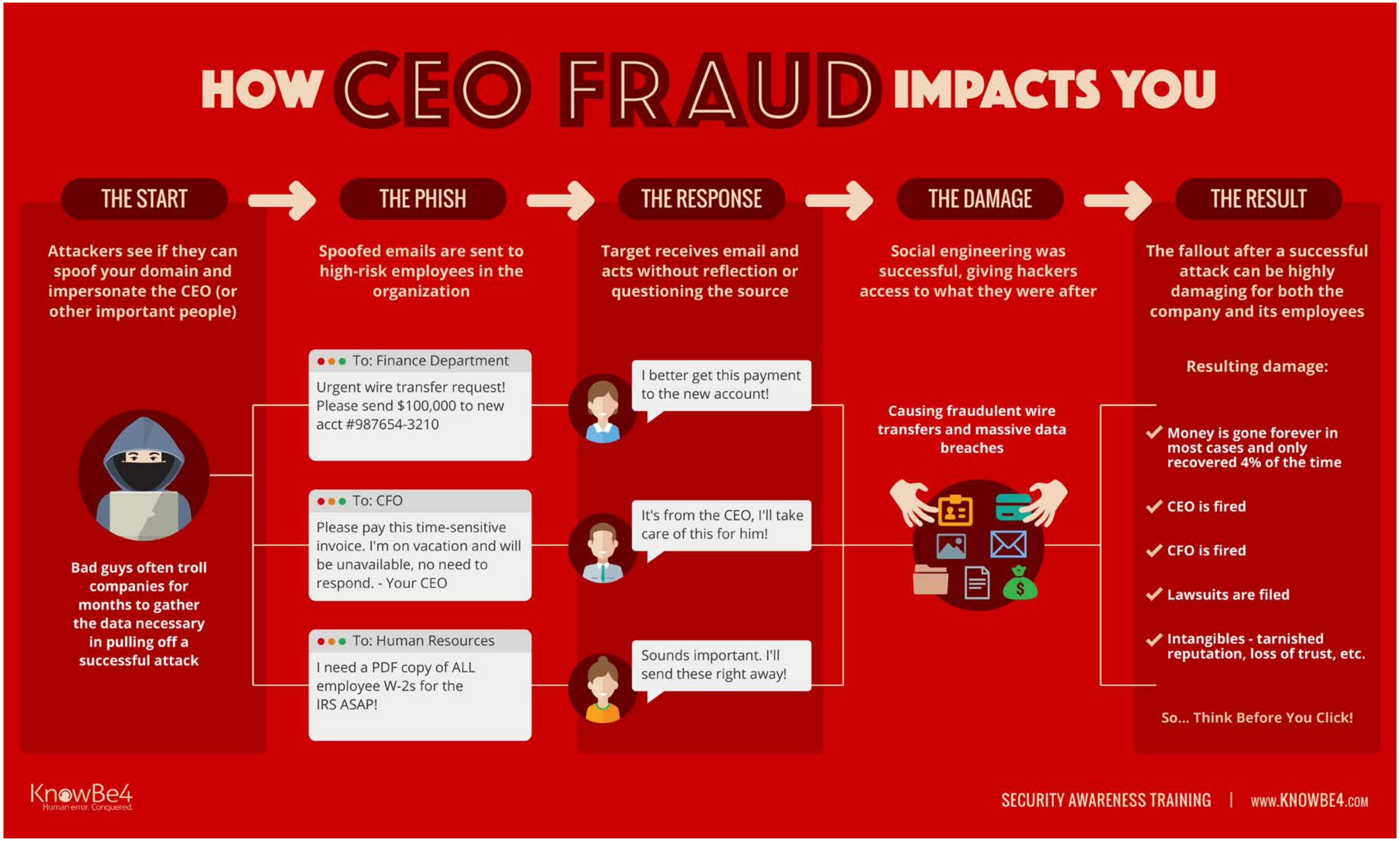
Send $300 worth of bitcoin to this address:

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Ransomware - Safeguards

- **Protect the keys**
  - **Strong passwords (14+ characters, mixed with upper, lower, numbers, special characters)**
  - **Two factor authentication**
- **Train staff to detect and report suspicious behaviors**
- **Train staff not to do “dumb stuff”**
- Back up computers
  - Store backups separate from the network, off site
  - Test back ups
- **Consider cyber liability / cyber crime insurance**
- **Have an incident response plan**
  - **Who to call**
  - **What to do**

CEO Fraud



HOW CEO FRAUD IMPACTS YOU

THE START

Attackers see if they can spoof your domain and impersonate the CEO (or other important people)

Bad guys often troll companies for months to gather the data necessary in pulling off a successful attack

THE PHISH

Spoofed emails are sent to high-risk employees in the organization

To: Finance Department
Urgent wire transfer request! Please send $100,000 to new acct #987654-3210

To: CFO
Please pay this time-sensitive invoice. I'm on vacation and will be unavailable, no need to respond. - Your CEO

To: Human Resources
I need a PDF copy of ALL employee W-2s for the IRS ASAP!

THE RESPONSE

Target receives email and acts without reflection or questioning the source

I better get this payment to the new account!

It's from the CEO, I'll take care of this for him!

Sounds important. I'll send these right away!

THE DAMAGE

Social engineering was successful, giving hackers access to what they were after

Causing fraudulent wire transfers and massive data breaches

THE RESULT

The fallout after a successful attack can be highly damaging for both the company and its employees

Resulting damage:

- ✓ Money is gone forever in most cases and only recovered 4% of the time
- ✓ CEO is fired
- ✓ CFO is fired
- ✓ Lawsuits are filed
- ✓ Intangibles - tarnished reputation, loss of trust, etc.

So... Think Before You Click!

KnowBe4
Human error. Conquered.

SECURITY AWARENESS TRAINING | www.KNOWBE4.com

CEO Fraud - Safeguards

- **Protect the keys**
  - **Strong passwords (14+ characters, mixed with upper, lower, numbers, special characters)**
  - **Two factor authentication**
- **Train staff to detect and report suspicious behaviors**
- **Train staff not to do "dumb stuff"**
- Talk to your bank and implement security on your accounts
- Create documented internal controls (for wire transfers, gift card purchases, W2 / payroll changes, etc.)
- Executives should refrain from being over active on social media
- **Consider cyber liability / cyber crime insurance**
- **Have an incident response plan**
  - **Who to call**
  - **What to do**

Threat Focused Defense Isn’t Enough

Attack Techniques

- Phishing
- Spear phishing
- Whale phishing
- Botnets
- Distributed denial-of-service (DDoS)
- Hacking
- Malware
- Pharming
- Phishing
- Ransomware
- Ransacking
- Spam
- War driving
- War dialing
- Web defacement
- Distributed Malware Attacks

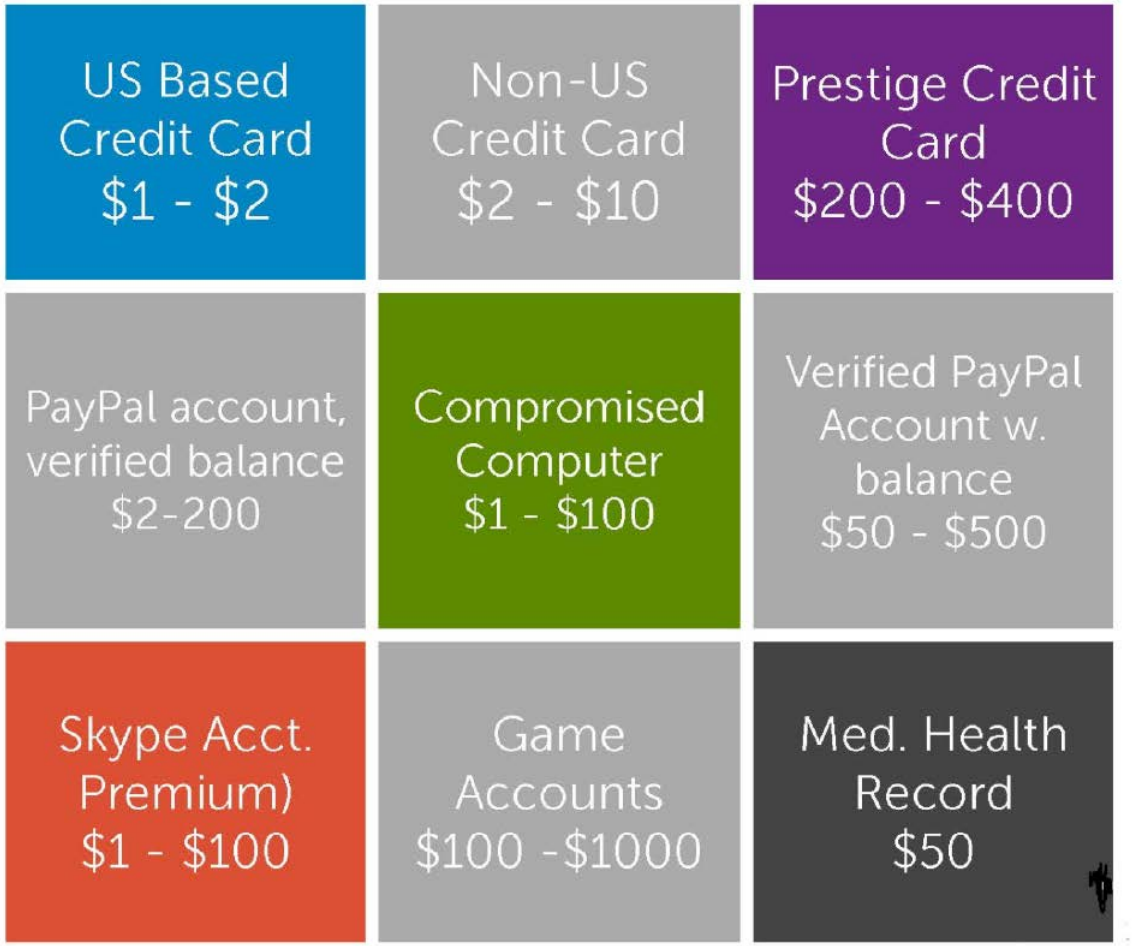
Threat focused is “security minded” not risk focused.

Techniques change over time. As defenders secure against a technique a new technique evolves to take its place.

“We build a 10 foot wall and the hackers build an 11 foot ladder.”

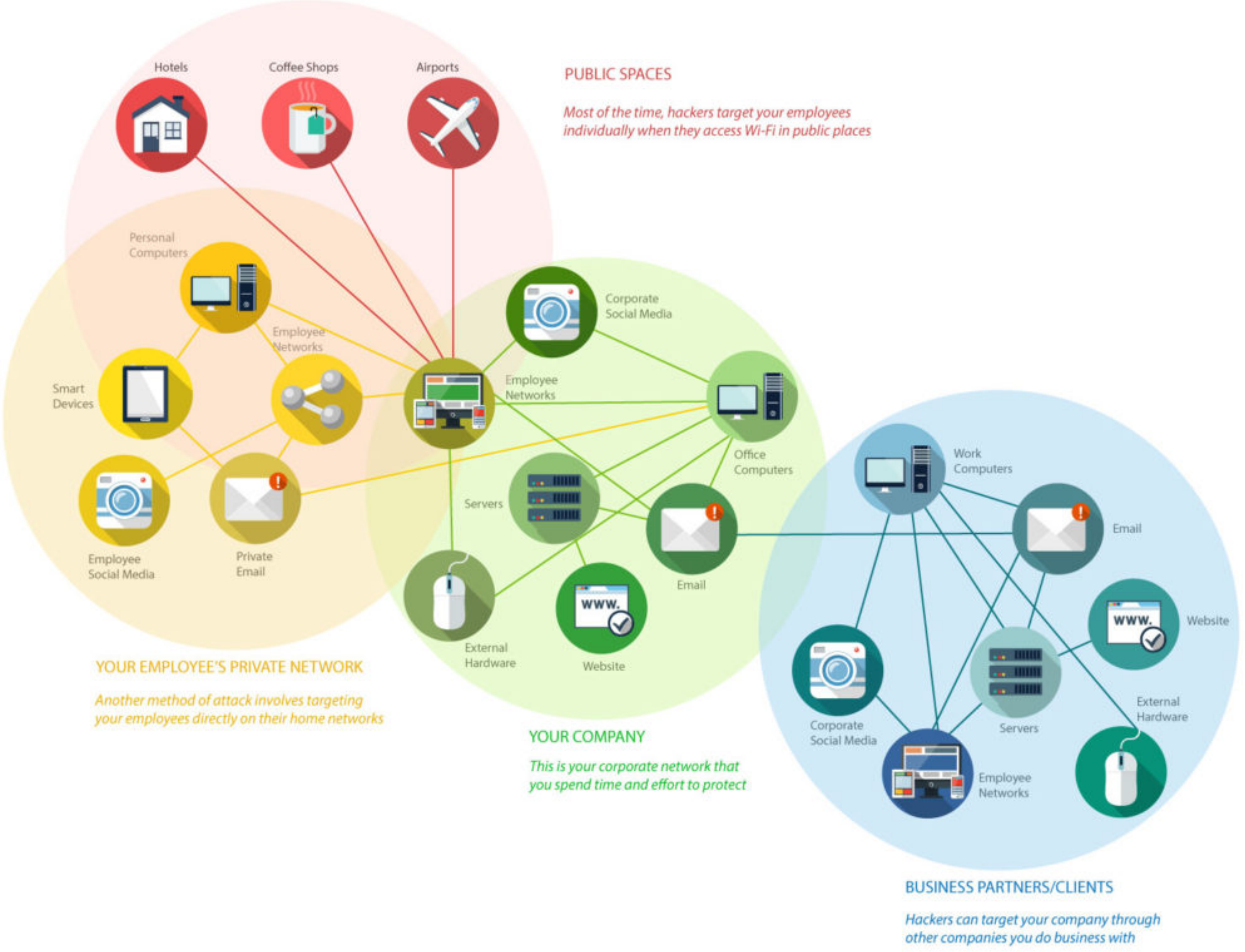
Focusing only on technique will lead us astray.

Business Impact: It’s all about the money!



US Based Credit Card $1 - $2	Non-US Credit Card $2 - $10	Prestige Credit Card $200 - $400
PayPal account, verified balance $2-200	Compromised Computer $1 - $100	Verified PayPal Account w. balance $50 - $500
Skype Acct. Premium) $1 - $100	Game Accounts $100 -$1000	Med. Health Record $50

Digital Assets Present Huge Attack Surface



PUBLIC SPACES

Most of the time, hackers target your employees individually when they access Wi-Fi in public places

YOUR EMPLOYEE'S PRIVATE NETWORK

Another method of attack involves targeting your employees directly on their home networks

YOUR COMPANY

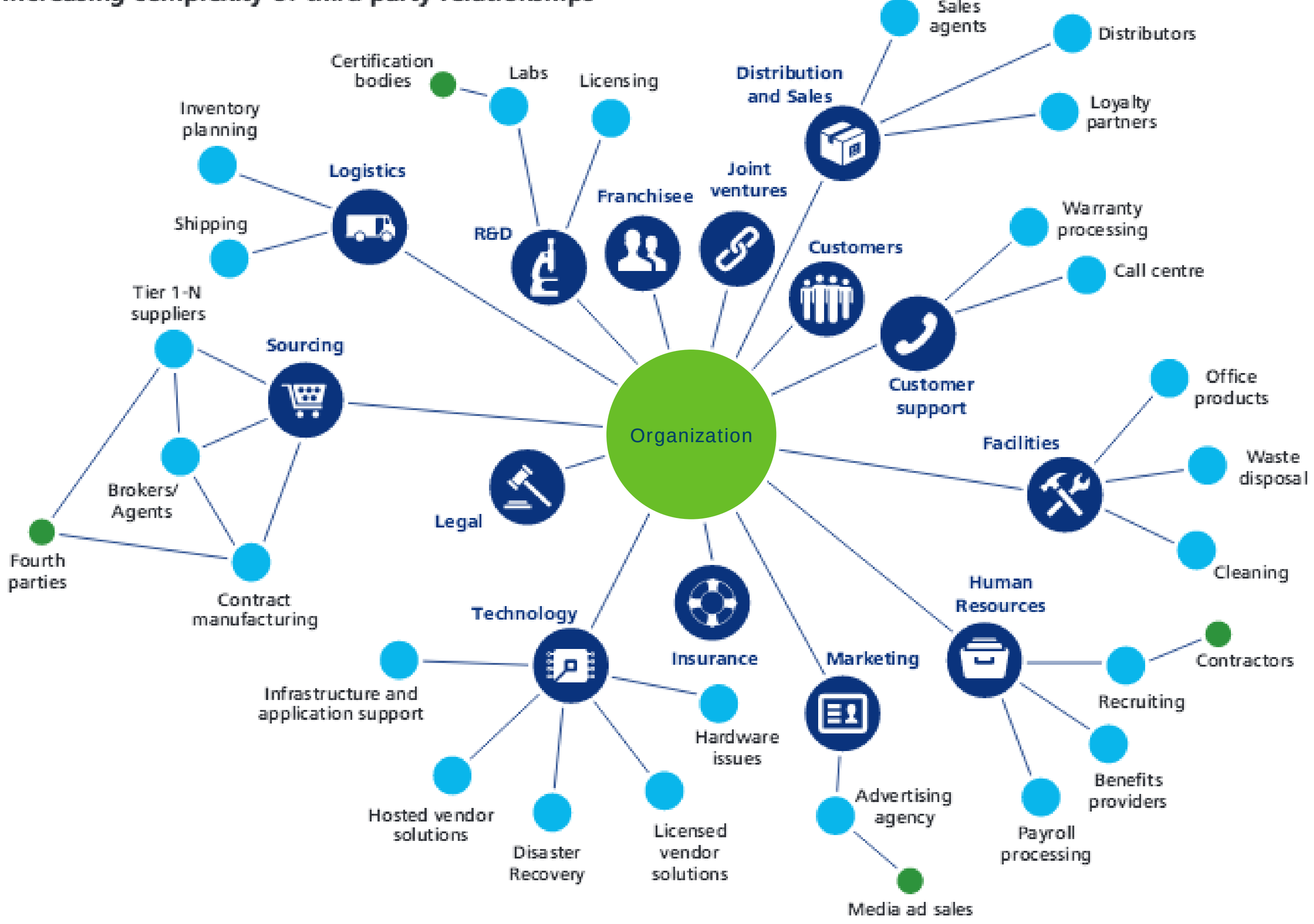
This is your corporate network that you spend time and effort to protect

BUSINESS PARTNERS/CLIENTS

Hackers can target your company through other companies you do business with

Vulnerability: Your Third Parties

Increasing complexity of third party relationships



Organization

Logistics
Inventory planning
Shipping

R&D
Certification bodies
Labs
Licensing

Franchisee

Joint ventures

Distribution and Sales
Sales agents
Distributors
Loyalty partners

Customers

Customer support
Warranty processing
Call centre

Facilities
Office products
Waste disposal
Cleaning

Human Resources
Contractors
Recruiting
Benefits providers
Payroll processing

Marketing
Advertising agency
Media ad sales

Insurance

Technology
Infrastructure and application support
Hosted vendor solutions
Disaster Recovery
Licensed vendor solutions
Hardware issues

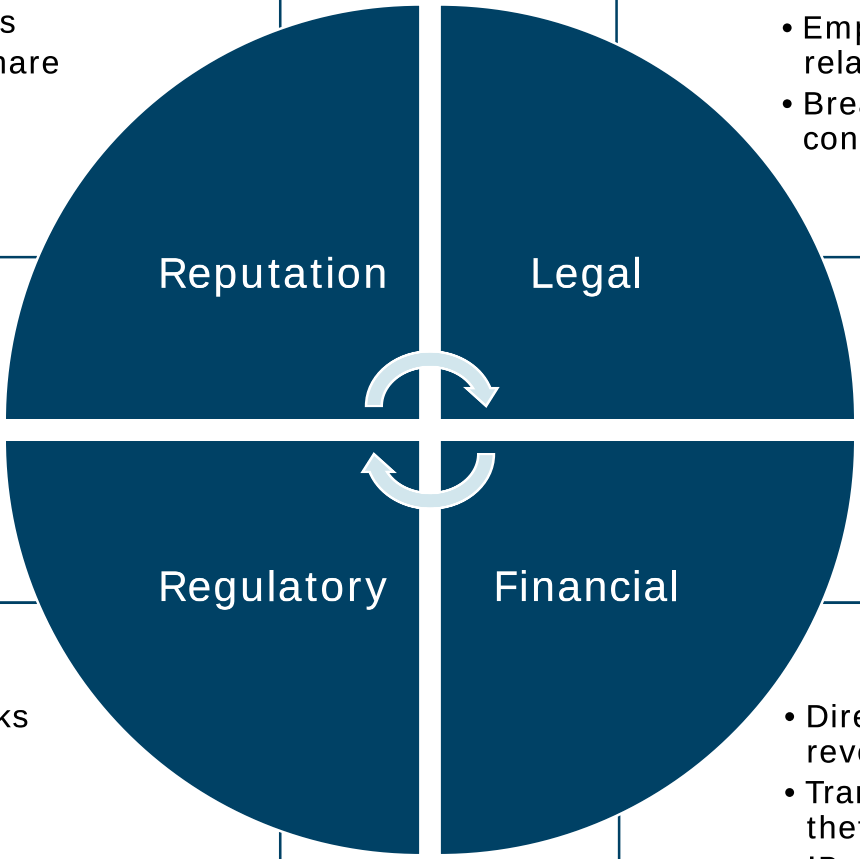
Legal

Sourcing
Tier 1-N suppliers
Brokers/ Agents
Contract manufacturing
Fourth parties

Impact: Potential Business Losses

- Clients / customers
- Market share

- Civil damages
- Employment related suits
- Breach of contract



Reputation

Legal

Regulatory

Financial

- Claw backs
- Fines
- Penalties

- Direct loss of revenue / cash
- Transactional theft
- IP devaluation

Impact: Cost of a data breach

Cost per record	
Global Average	
$158	+15% since 2013

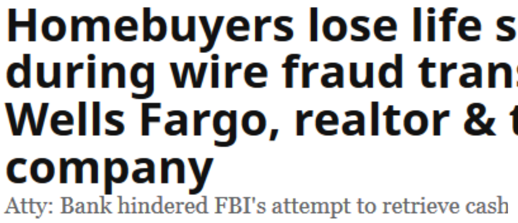
Cost per incident	
Global Average	
$4M	+29% since 2013

Highest Countries	Lowest Countries
$221 United States	$100 Brazil
$213 Germany	$61 India

Highest Countries	Lowest Countries
$7M United States	$1.8M Brazil
$5M Germany	$1.6M India

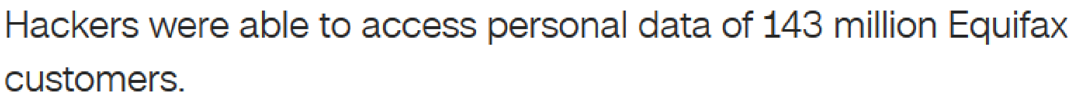
Source: https://www.ibm.com/security/data-breach/

What’s the Worst That Can Happen?

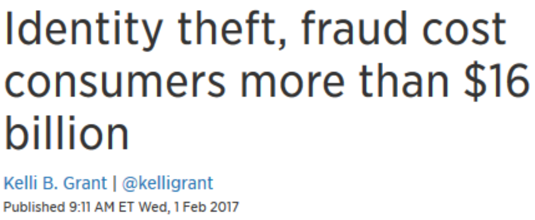


Homebuyers lose life savings during wire fraud transaction, sue Wells Fargo, realtor & title company

Atty: Bank hindered FBI's attempt to retrieve cash



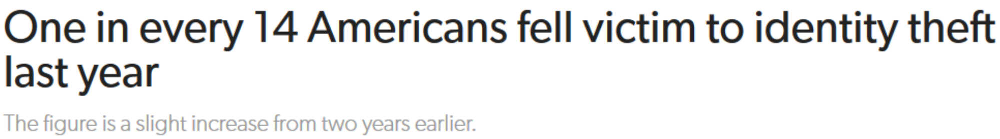
Hackers were able to access personal data of 143 million Equifax customers.



Identity theft, fraud cost consumers more than $16 billion

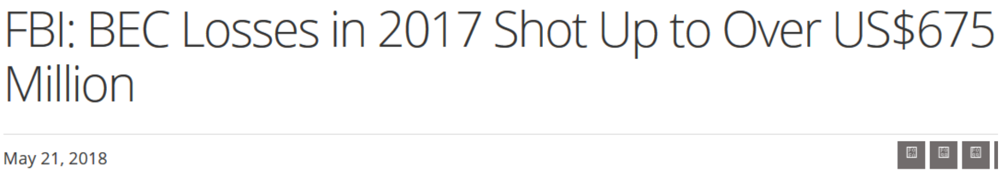
Kelli B. Grant | @kelligrant

Published 9:11 AM ET Wed, 1 Feb 2017



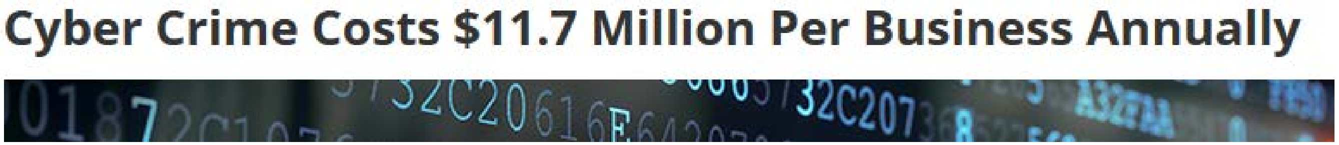
One in every 14 Americans fell victim to identity theft last year

The figure is a slight increase from two years earlier.



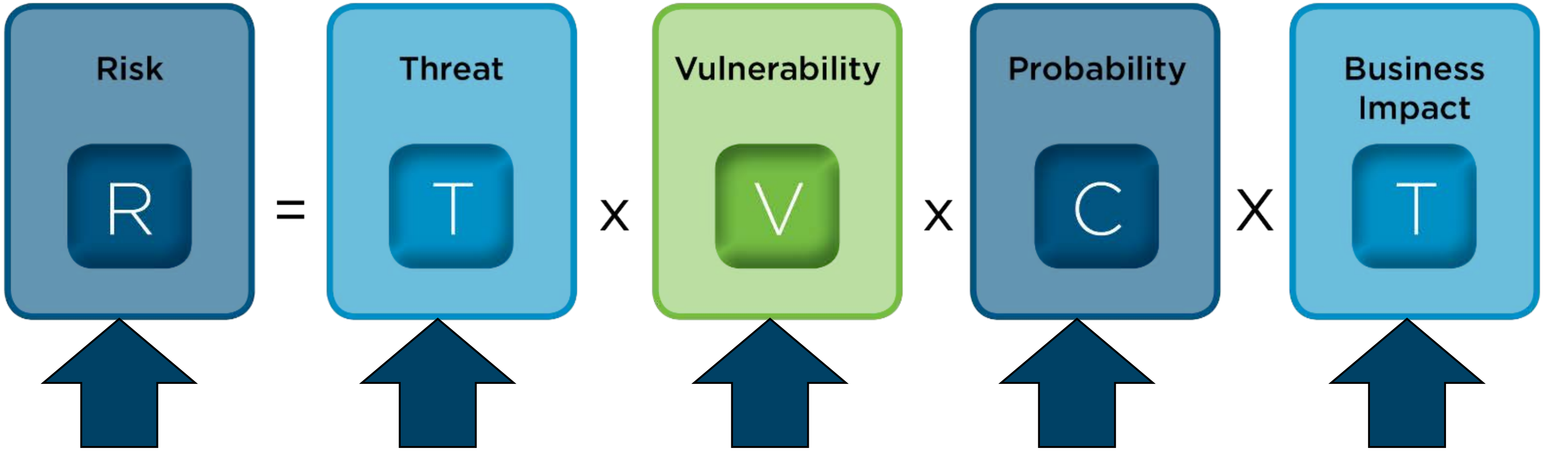
FBI: BEC Losses in 2017 Shot Up to Over US$675 Million

May 21, 2018



Cyber Crime Costs $11.7 Million Per Business Annually

Cyber Risk Rising



Security is a business issue

Compliance with cybersecurity standards does not ensure security & resiliency

Blurring of cyber threat actors nation-states & organized crime

Bad actors have monetized cybercrime

Attacks evolve as vulnerabilities are safeguarded

Attack surface is expanding

Shortage of Experienced Cybersecurity Professionals

Not executing on removing vulnerability especially in information handling & communication channels

Business Email Compromise on the rise

Ransomware on the rise

Email and other human resource based attacks on the rise

Higher cost of cyber data breaches

Real revenue interruptions

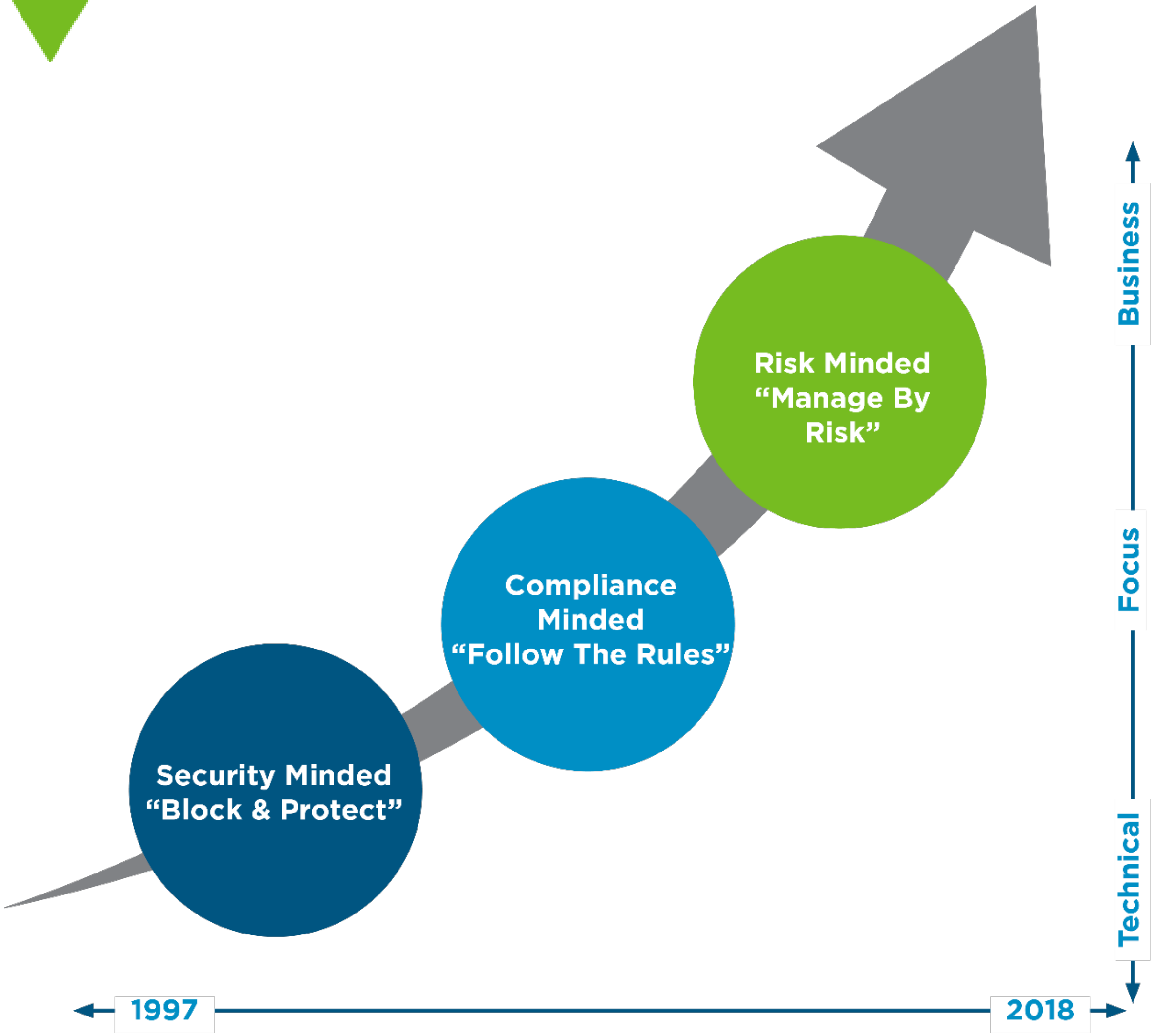
Cash being stolen directly

Safety rising as an issue

Higher cyber liability insurance premiums

Protecting Your Business

Cybersecurity over time



Security Minded Phase was about "keeping them out"

Compliance Minded Phase was about "checking the box"

Risk Minded Phase is about measuring and managing risk to build resiliency

We Don’t Play Football Without A Playbook ……….

Woody Hayes’ Playbook

Playbook from his last season as coach — features diagrams of formations, reminders of points he wanted to make to assistant coaches and things to emphasize at team meetings, such as “Get to bed early tonight,” “Start fast” and “Never let up.” It was not sheer luck or natural talent that made Hayes so successful. In his speech at the 1986 winter commencement, he shared his strategy regarding those who were smarter: “They couldn’t outwork me,” he said.

Source: OSU.edu

Get organized – Ohio Data Protection Act

- Provides an affirmative defense in the case of a breach involving “restricted information”
- Requires a firm to be “substantially compliant with one of 7 frameworks
- PCI is NOT on the list
- Management and IT (InfoSec) work to collaboratively select a framework or frameworks to provide “defense in depth” based on a risk assessment

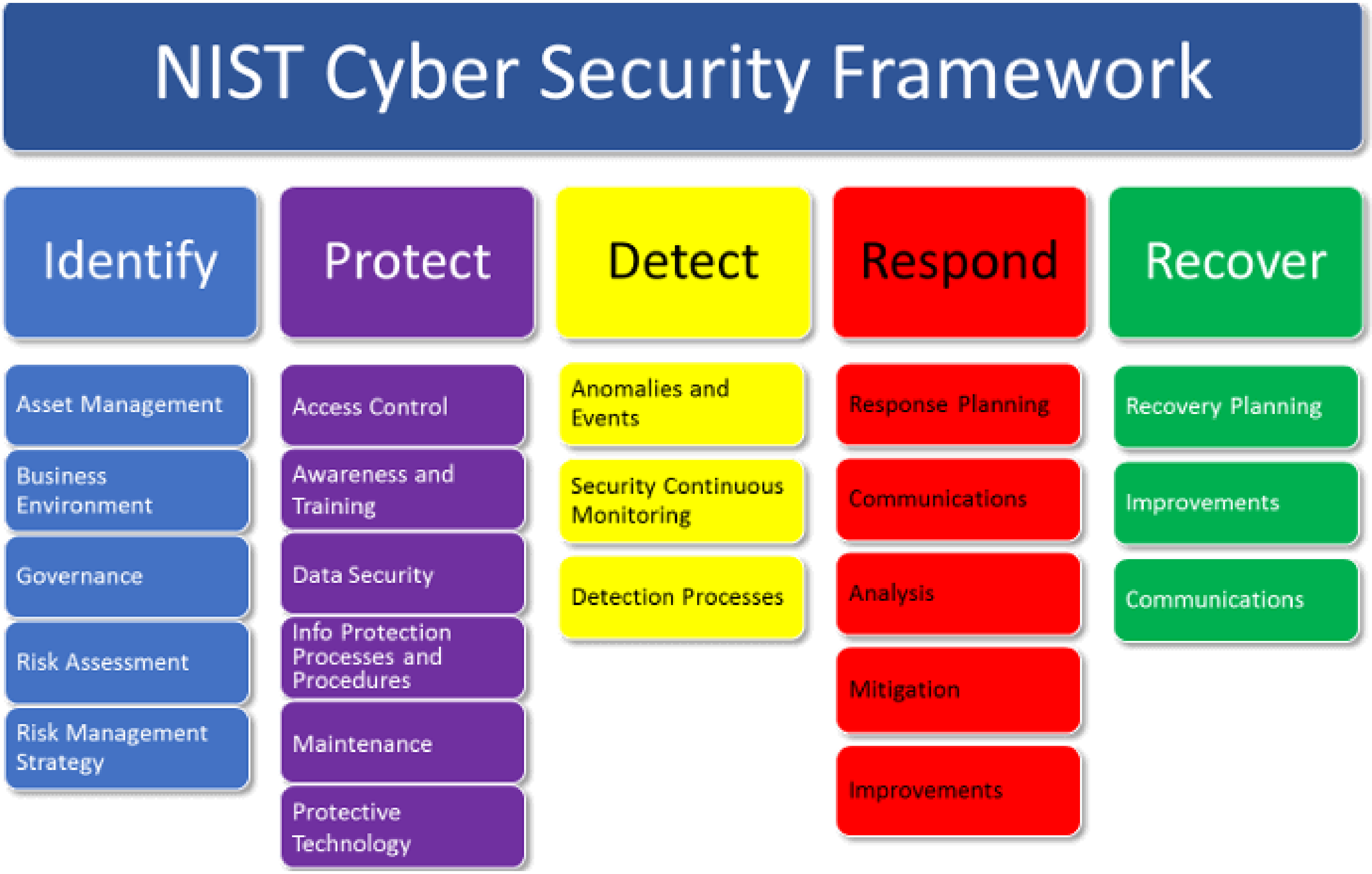
Ohio Data Protection Act Frameworks:

- **NIST Cyber Security Framework (NIST CSF)**
- NIST 800-171
- NIST 800-53 / NIST 800 53a
- FedRamp
- **Center for Internet Critical Security Controls (CIS 20)**
- ISO / IEC 27000
- HIPAA / HITECH
- Gramm – Leach – Bliley (GLBA)

Consider Cybersecurity Business Perspective

- Inventory your digital assets – across entire “attack surface”
- Management (NOT IT) should select a cybersecurity framework(s) from which to organize cybersecurity defenses at a business level
- Talk to your bank about protecting financial transactions
- Review cybersecurity coverage
  - Are all transaction activities covered?
  - Does the policy provide affirmative defenses?
  - Does the policy provide incident response support?
- Inventory cybersecurity obligations to your customers / clients
  - Regulatory obligations
  - Contractual obligations
- Measure & manage the risks vendors and suppliers present to your firm

Adopt and Follow Cybersecurity Framework

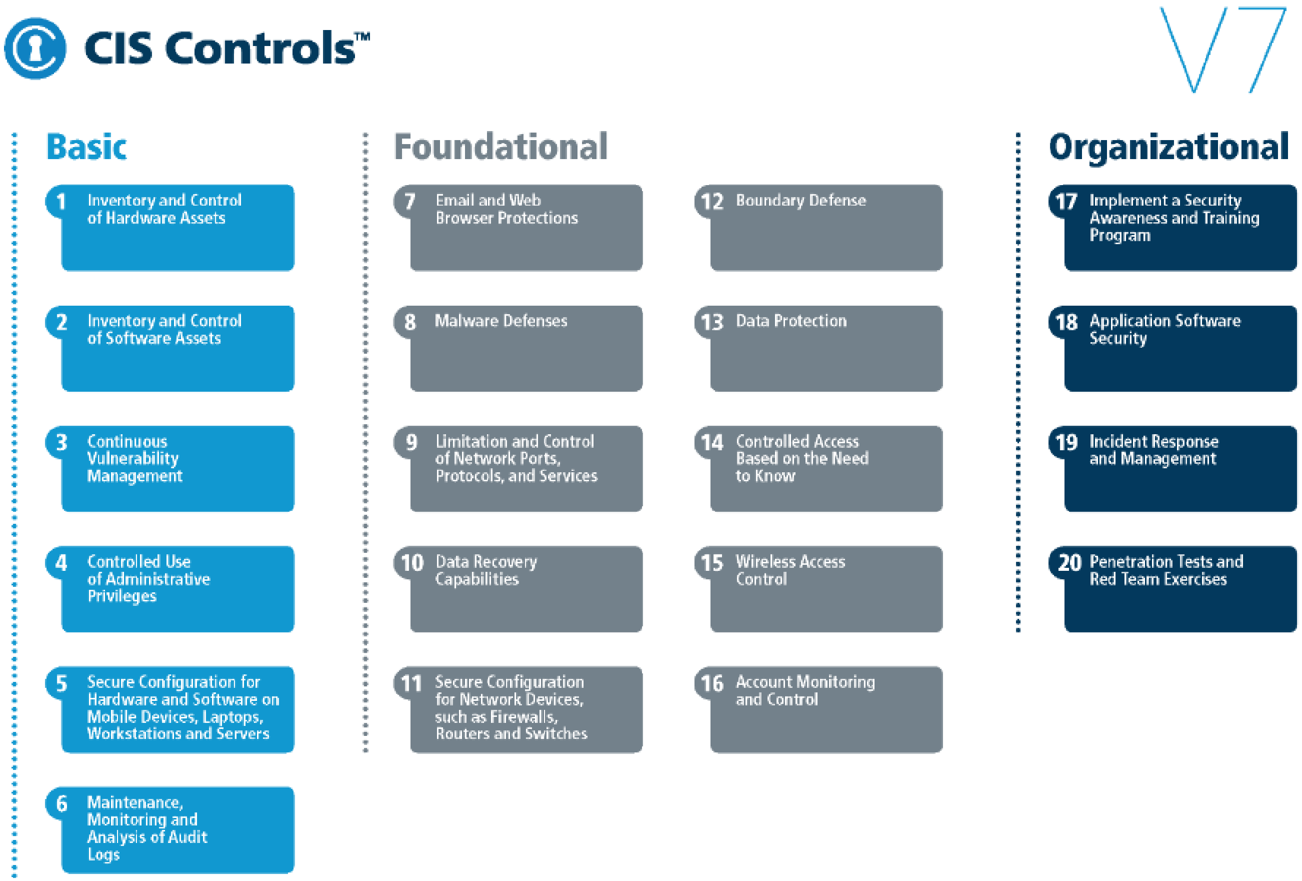


NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

National Institute of Science and Technology (NIST) Cybersecurity Framework (CSF)
https://www.nist.gov/cyberframework

Adopt and Follow Cybersecurity Framework



CIS Controls™ V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Center for Internet Security (CIS) **Critical Security Controls (CIS 20)**
https://www.cisecurity.org/controls/

Control Framework Recommendation

- Unless regulatory authority or client obligations requires another framework we advocate using NIST CSF and CIS 20 in combination
  - NIST CSF is more business oriented
  - CIS 20 is more technically prescriptive
  - Both scale to the size and maturity of the business

- If a regulatory obligation, (i.e. HIPAA, PCI, NIST 800-53, FEDRAMP, etc.) we advise using NIST CSF / CIS 20 as foundation for program

- Almost all frameworks can be “cross walked” in NST CSF and CIS 20

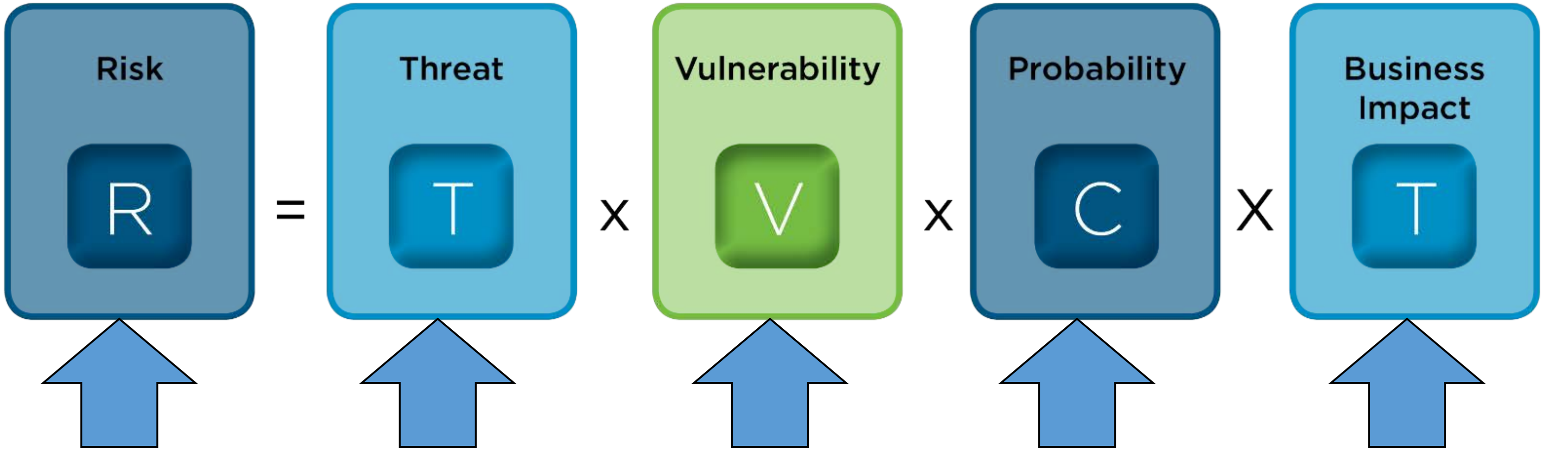
Before the Breach – Test!

- Conduct **Independent Assessment**
  - Independent risk assessment – using your selected framework -- including vulnerability assessment of network and cloud infrastructure
  - Conduct an email cyber risk assessment
  - If you use a third party IT provider, assess their work against their contract
  - Independent adversarial penetration test of enterprise NOT just external network
- Provide **Cybersecurity Awareness Education and Training** programs for all employees to develop a real cybersecurity culture
  - Include information handling training for employees handling protected information and cash
- **Business Continuity / Disaster Recovery Plan / Incident Response**
  - Document an full scope plan
  - Test back up and other recovery systems regularly
  - Test the incident response plan annually with a table top test
- Conduct a **Cyber Liability Insurance Coverage** adequacy evaluation to discover what is covered and what is not covered, and understand the cost of cybersecurity remediation actions vs. the cost of the cyber insurance premium

COVID-19 Cyber Issues

- Create an organizational culture of cybersecurity from the top down
  - Raise security awareness with employees
  - Avoid email based financial transactions
- Harden computer network components
  - Quick change to remote working posture creates weaknesses
  - Focus IT resources on securing the remote network
- Continue Security Testing
  - Prioritize critical systems
  - Understand how operating changes impact compliance programs
  - Speak to vendors / third parties about their testing
- Monitor IT assets and employees
- Plan for more bad news
  - Review Incident Response Plans
  - Review / test disaster recovery plans

Cyber Risk Rising



Risk will be elevated throughout the pandemic

Bad actors using COVID-19 themed attacks to conduct BEC, ransomware, Denial of Service

Attack surface rapidly expanded with work from home / remote connections in support of social distancing

IT staffs are spread thin

IT staffs are supporting users with weaker skills and inadequate tools

FBI, FTC, Homeland Defense all have published advisories on COVID-19 themed attacks

Electronic storefronts, pone, email systems are most businesses only way to serve customers

Weak cAash flow positions for many firms will magnify a cyber event's impact

Questions?