Cybersecurity and Data Breach Response

Moderator:

Ben Johnson, Director of Risk Management, Cornerstone Support

Panelists:

Xerxes Martin, founding partner of Malone Frost Martin PLLC

Dr. Michael Owens, Information Security Officer/Global Security for Equifax

RMAi
RECEIVABLES MGMT. ASSOC. INTL.
SETTING THE GLOBAL STANDARD

Receive Conference Text Alerts

TEXT

RMAI

to 77513 🇺🇸
to 23456 🇨🇦
to 351927946968 🌍

Conference text messaging sponsored by

solutions by text™

2020 ANNUAL CONFERENCE
BRINGING THE INDUSTRY INTO FOCUS

Access This Presentation

TEXT

CYBER

to 77513 🇺🇸

to 23456 🇨🇦

to 351927946968 🌍

Conference text messaging sponsored by

solutions by text™

Disclaimer

This information is not intended to be legal advice and may not be used as legal advice. Legal advice must be tailored to the specific circumstances of each case.

Every effort has been made to ensure this information is up-to-date. It is not intended to be a full and exhaustive explanation of the law in any area, nor should it be used to replace the advice of your own legal counsel.

Any opinions expressed are the opinions of the speaker and not their organization, or the Receivables Management Association International.

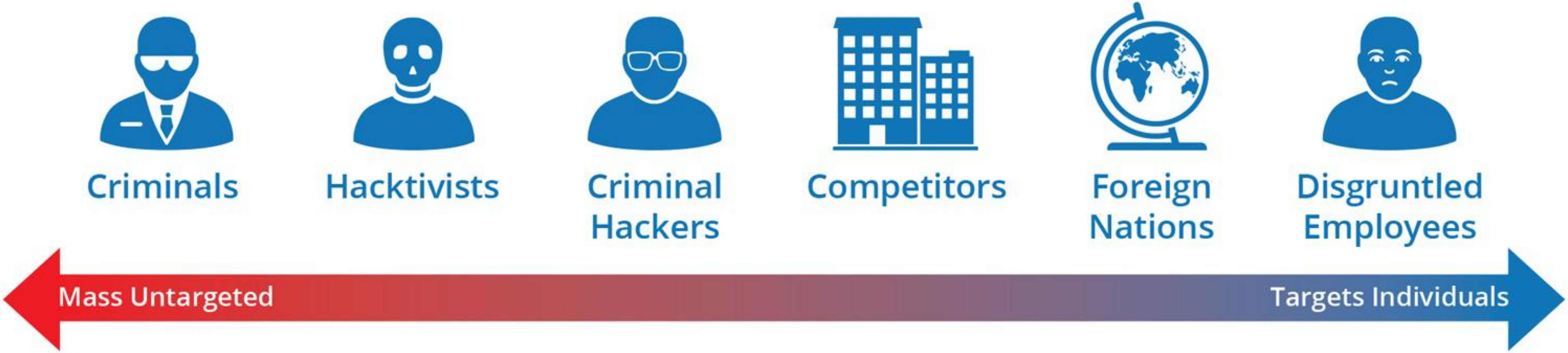
Common types of data breaches

- Information theft
- Ransomware
- Password guessing
- Key stroke recorders
- Phishing
- Malware or virus
- Denial-of-Service

Why would they hack us?

Why not target consumers with money and good credit?

Potential Adversaries



Criminals

Hacktivists

Criminal Hackers

Competitors

Foreign Nations

Disgruntled Employees

Mass Untargeted

Targets Individuals

Sharks in the water:
Will this breach result in a lawsuit?

- Size of the company
- Number of individuals effected
- How many times data incidents have occurred
- Preventability of the incident
- Type of records - Minors/Elderly, SSN, Financial, healthcare info
- What to do? Federal and state privacy laws

The worst breaches in history (so far)

- Breaking News: LifeLabs® **, Jan 2020**
- Canadian medical diagnostics company – almost 50% of Canada’s population has had some sort of testing done by the company as part of their normal health care
- Class action could result in over $1 BILLION in exposure.

The worst breaches in history (so far)

- **10 of the 15 worst breaches in history occurred in just the past decade**

(Source: Business Insider)

One example is the yahoo! incident in 2013-2014

- Hackers exposed **over 3 BILLION** user accounts
- Verizon was in talks to purchase Yahoo at the time; the breach ultimately dropped Yahoo’s valuation by $350 MILLION.

*There is speculation that a state actor perpetrated the Yahoo breach

The worst breaches in history (so far)

- Marriott INTERNATIONAL, **2014-2018**
- In 2014 Hackers infiltrated Starwood's systems undetected, and Marriott purchased Starwood in 2016. The hackers remained in the Marriott/Starwood systems for FOUR YEARS between 2014 and 2018.
- Stole data of 500 million customers- contact info, passport #s, rewards numbers and credit card info.
- Practical note- when you acquire a new entity, THOROUGHLY screen the new entity's systems before integrating them into your own.

Other significant breaches include:

- AdultFriendFinder® (2016) - 412 M accounts exposed
- Heartland Payment Systems (2009) - 134 M credit card numbers stolen; paid $145 M in compensation
- TARGET (2014) – Lost PII of 110 M customers. Cost $162 M
- facebook , ebay , FIRST AMERICAN First American Title™ , and more

HOARDING Old Records

- Microsoft recently exposed 250 million records due to a cloud misconfiguration; call recordings dating back 14 years
- Capitol One breach in 2019 included 100M credit card apps dating back to 2005
- **Why aren’t we archiving or unplugging old records?**

BIPA, HIPAA, and other damage multipliers

- BIPA: Biometric Information privacy Act (Illinois):
  - Facial recognition, thumbprint scans
  - Requires reasonable care to safeguard
  - $1000 negligence / $5000 intentional PER VIOLATION (massive implications for class actions!)
- HIPAA:
  - Mandatory breach notification; class actions and civil enforcement penalties
  - Quest Diagnostics and LabCorp (2019) – over 20 million combined victims
- CCPA: California Consumer Privacy Act (upcoming)
  - Includes exception for sale of PI to consumer reporting agency to generate consumer report under FCRA

EQUIFAX FCRA suit

- Breach compromised data of 143 Million consumers
- Because the data was stolen, and not technically “furnished” by Equifax, the exposed data did not constitute a “consumer report,” and thus was not subject to FCRA liability.
- Still had liability under other statutes

Equifax: Lessons Learned Security and Risk Management

Best practices to put in place <u>BEFORE</u> an incident happens:

- Ensure **risk management** is fully understood throughout the organization – ask external experts to assess your current risk governance
- Re-evaluate the strength of your **control environment** on a regular basis and continuously implement improvements to shore up each line of defense – test your controls and do not just rely on surveys and scorecards
- Leverage a **zero trust approach**, meaning do not assume your assets are secure – run multiple backups and have visibility into your environments in all ways possible – explain this concept to staff in layman's terms and use examples

Equifax: Lessons Learned Security and Risk Management

Best practices to put in place <u>BEFORE</u> an incident happens:

- Invest in **detection,** not just prevention – use multiple vendors, create overlap in scanning
- Increase **Board attention** to cybersecurity risks / trends, the Company's approach to managing those risks, and cybersecurity as a strategic component of the Company's business
- Make sure that the **CISO** has a seat at the table

Equifax: Lessons Learned Security and Risk Management

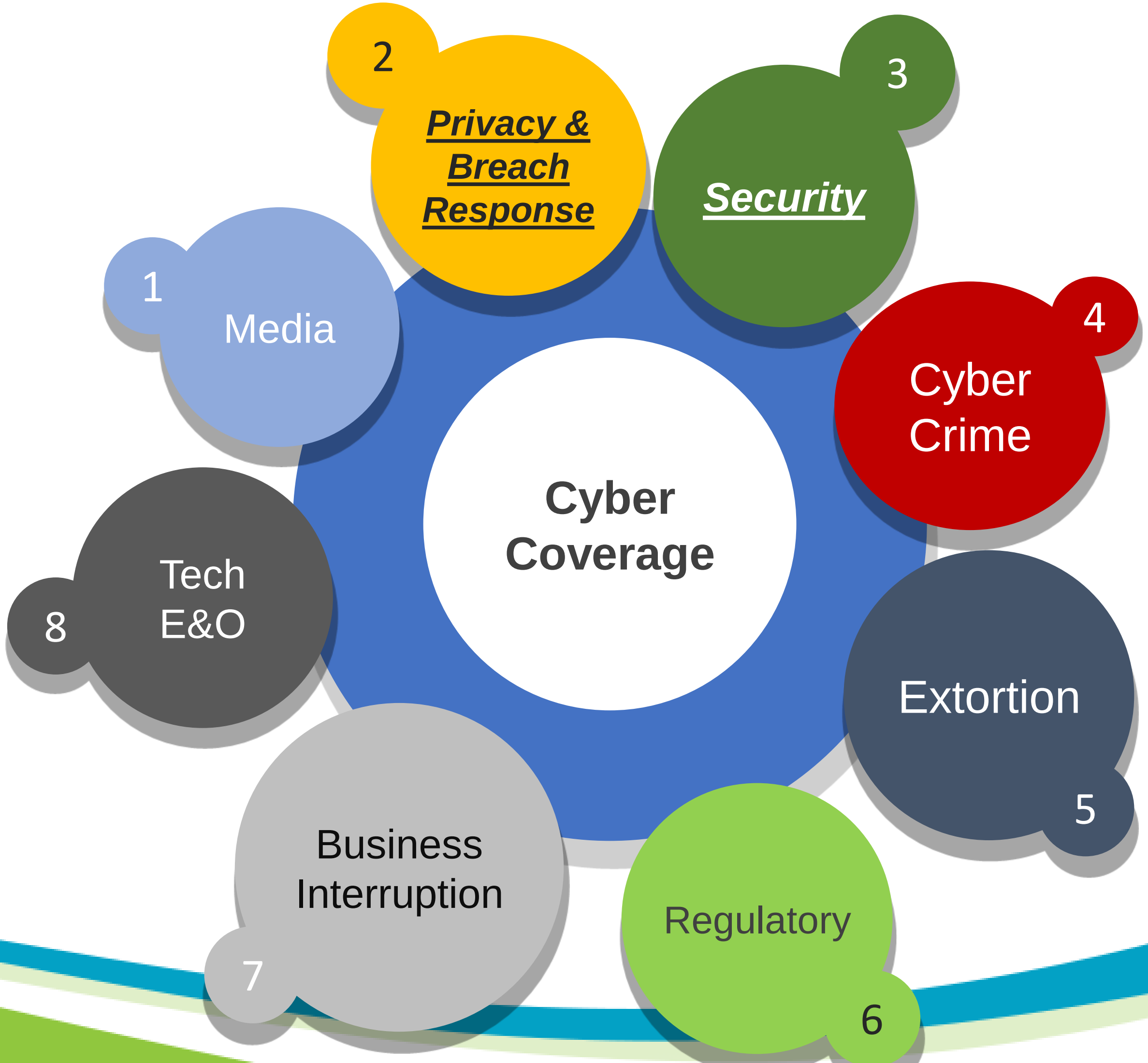
Best practices to put in place BEFORE an incident happens:

- **Stress test** your organization and your approval process via real-world, worst-case simulations – be specific and create actionable scenarios to practice – include everyone (sales reps, system admins, ISOs, etc.)
- Identify **all external support** needed ahead of time – critical vendors, suppliers, consulting firms, operations support, etc. – include them in your simulations and stress tests
- Ensure that you also include **international teams** in stress tests, weighing translation needs and in-country resources
- Be sure to lay out the distribution of **decision-making authority** between the international market and HQ

Recent Data Privacy Precedent

- *Resmick v. Avmed* (11th Cir. 2012)
- *In re adobe Sys. Privacy Litigation* (N.D. Cal. 2014)
- *Tabata v. Charleston Area Med. Ctr.* (W. Va. 2014)
- *Remijas v. Neiman Marcus Group* (7th Cir. 2015)
- *Spokeo Inc. v. Robins* (2016)
- *Levert v. P.F. Changs China Bistro* (7th Cir. 2016)
- *Attias v. Carefirst Inc.* (D.C. Cir. 2017)

Cyber liability/data breach insurance



Coverage is customizable
First-party and third-party coverages

First vs. Third party coverage

- First-party costs include any expenses of the company directly related to the breach including state regulated notification costs, reputation management, legal and network investigation costs, and the loss of income during a breach. Third-party costs cover expenses incurred from outside the company and may include legal defense, settlements, and regulatory fines and penalties.

```
* Welcome to CityPower Grid Rerouting *

Authorised Users only!

New users MUST notify Sys/Ops.

login:
```

```
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
```

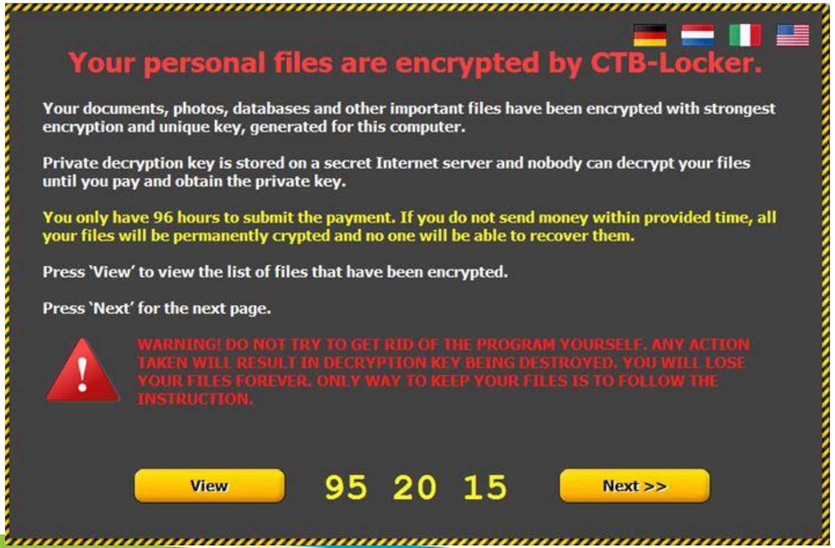
```
--- 10.2.0.0 ping statistics ---
1 packets transmitted, 1 packets received, +44 duplicates, [illegible] packet loss
round-trip min/avg/max/stddev   0.252/2.455/17.0/0/3.[illegible]
# ping  c 2 10.2.0.0 | grep '^64' | awk '{print "n[illegible]$[illegible]"}' | sed
  's.:.,g' | csh |& grep Address
Address:  10.2.1.3

# nmap  v  sS  O 10.2.1.3

Starting nmap V. 2.5NBETA25
Host 10.2.1.3 appears to be up [illegible]
Initiating SYN Stealth Scan against 10.2.[illegible]
For OSScan assuming that port [illegible] is open [illegible] port 1 is closed and neither are
firewalled
Insufficient responses [illegible] fingerprinting (3), OS detection may be less
accurate
Interesting ports [illegible] 10.2.[illegible]
(The 1521 ports [illegible] shown below are in state: closed)
Port       St[illegible]     Service
21/tcp     op[illegible]     ftp
22/tcp     op[illegible]     [illegible]
23/tcp     open              telnet
25/tcp     open              smtp
```

Breach Response can involve various factors

Insurance policy may provide for:

- ✓ Crisis Management
- ✓ Forensic Analysis
- ✓ Notification & Credit Monitoring
- ✓ Regulatory Coverage for Fines and Penalties

```
* Welcome to CityPower Grid Rerouting *

Authorised Users only!

New users MUST notify Sys/Ops.

login:

rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL

--- 10.2.0.0 ping statistics ---
1 packets transmitted, 1 packets received, +44 duplicates, [illegible] packet loss
round-trip min/avg/max/stddev   0.252/2.455/17.0/0/3.[illegible]
# ping  c 2 10.2.0.0 | grep '^64' | awk '{print "[illegible]"}' | sed
   's.:,,g' | csh |& grep Address
Address:  10.2.1.3

# nmap  v  sS  O 10.2.1.3

Starting nmap V. 2.5NBETA25
Host 10.2.1.3 appears to be up [illegible]
Initiating SYN Stealth Scan against [illegible]
For OSScan assuming that port [illegible] is open [illegible] port 1 is closed and neither are
firewalled
Insufficient responses [illegible] sequencing (3), OS detection may be less
accurate
Interesting ports [illegible] 10.2[illegible]
(The 1521 ports [illegible] shown below are in state: closed)
Port       St[illegible]      Service
21/tcp     ope[illegible]     ftp
22/tcp     ope[illegible]     [illegible]
23/tcp     open[illegible]    telnet
25/tcp     open               smtp

40                    1:501          56.18                   00:00.000
```



Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

95 20 15

How do I know if there has been a breach?

- Is there a virus detected?
- Has your system stopped working or are you locked out?
- Did you get a message stating your system is being held for ransom?
- Have your clients, vendors and business acquaintances reported an issue to you?

What do we do now?

With Insurance Coverage:

Contact the Insurer

For Preferred Vendor policy, pick one and work with them to determine:

How many records were lost?

Dates of breach?

Should you report?

How to fully document?

For Turnkey, appoint a liaison in your company to work with the carrier and they will handle everything.

Without Insurance:

Work with your IT professionals, HR Professionals

Find an experienced attorney

Questions?

RMAi
RECEIVABLES MGMT. ASSOC. INTL.
SETTING THE GLOBAL STANDARD

Access This Presentation

TEXT

CYBER

to 77513 🇺🇸
to 23456 🇨🇦
to 351927946968 🌍

Conference text messaging sponsored by
solutions by text™

2020 ANNUAL CONFERENCE
Bringing the Industry into Focus