February 14, 2017

Cyber Liability

Overview of Risks Facing Public Sector Entities

John Chino
Area Senior VP
Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Steve Robinson
Area President
RPS TECHNOLOGY & CYBER

Elissa Doroff
VP, Product Manager
XL CATLIN

Today’s Presenters

John G. Chino, ARM-PE, CSRM

ARTHUR J. GALLAGHER& CO. LEADERSHIP TEAM, PUBLIC SECTOR DIVISION

- Responsible for the development of Public Agency Risk Management Programs
- Completed two-year internship at AJG-UK office, first American to pass Lloyd’s Introductory Exam
- Instructor for The Institutes and faculty member of the National Alliance of Insurance Education and Research
- Board member of Community Matters 501(c)3

Steven R. Robinson

AREA PRESIDENT, RISK PLACEMENT SERVICES, INC.

- Leads national Technology & Cyber practice of RPS, a division of Arthur J. Gallagher & Co.
- Leads team of insurance professionals, developing cyber risk insurance programs in the following sectors: public entity, edu, finance, hospitality, technology, retail and others
- National speaker , educator and author in matters of cyber risk insurance
- B.A., University of South Carolina

Elissa Doroff

VICE PRESIDENT & PRODUCT MANAGER, CYBER & TECHNOLOGY, XL CATLIN

- Directs and manages XL Catlin’s risk management services designed to minimize the frequency and severity of data breachecs.
- Nearly a decade of cyber and technology insurance expertise as a claims counsel and broker
- National presenter on panels and seminars for clients and industry associations
- B.A., State University of New York at Albany
- Juris Doctor, Suffolk University Law School
- Admitted to practice law in Massachusetts and Connecticut

Today’s Topics

Overview of Risks Facing Public Entities

- Cyber Risk for Public Entities: COMMON PATTERNS, UNIQUE EXPOSURES
- What is Cyber Liability: HIGH-LEVEL OVERVIEW
- Fact Patterns of a Data Breach: 10 COMMON THREATS
- Active Cyber Claims We are Seeing: COVERAGE, PAYOUTS, ETC.
- Data Breach Prevention Overview: SIMPLE STEPS TO SHARE WITH ALL STAKEHOLDERS
- Breach Response & Incident Reporting: PROCESS, DO’S AND DON’TS
- Questions / Discussion

Cyber Risk for Public Entities

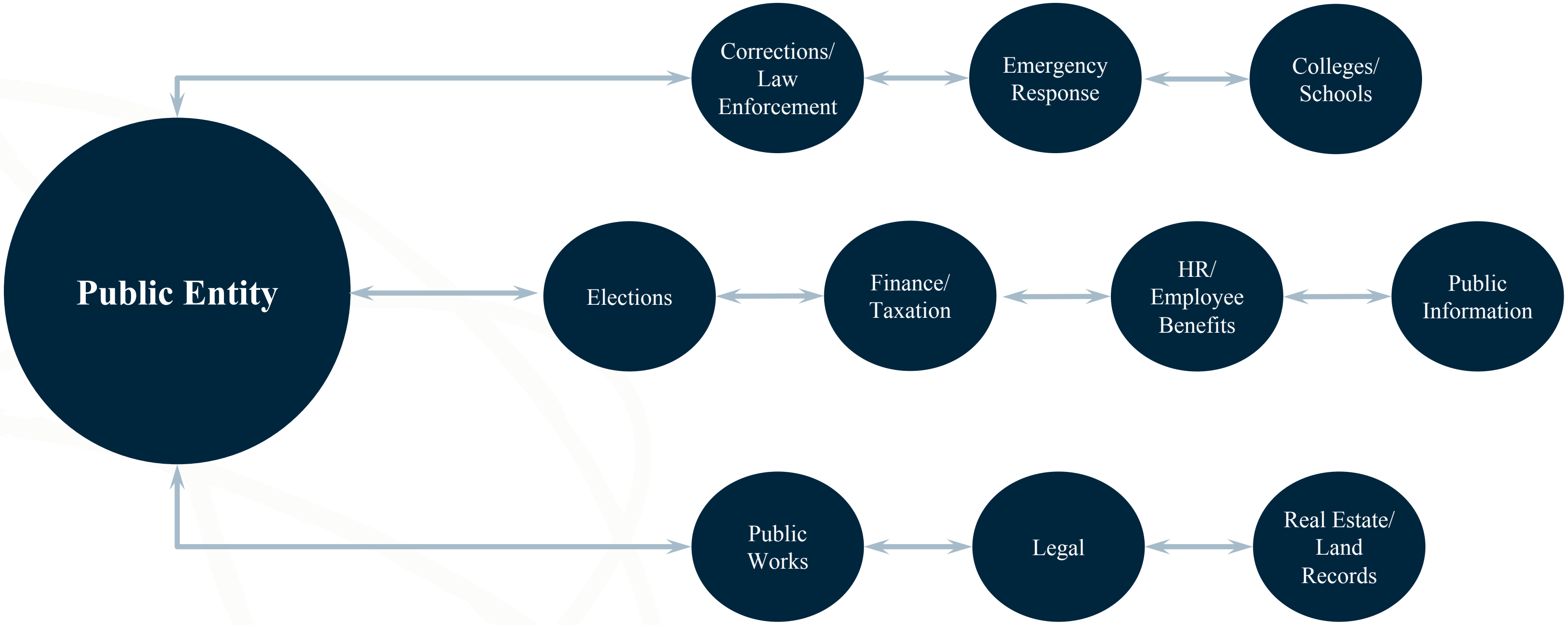
10 Fact Patterns of Data Breaches

- Missing or stolen laptop or storage device
- Mis-mailing
- Erroneous Data Posting
- Willful release based on fraudulent instruction (social engineering)
- Compromised System (Hacking)
- Loss or Theft of Physical Documents
- Lost Back-up Data or Tape
- Breach Caused by a Third-Party Vendor
- Improper Document/Equipment Disposal
- Insider

Source: IDT911

Public Entity Exposures

The Vast Array of Services Provided By Public Entities = Information Risk



Endless networks – some connected, some not – all containing valuable information that thieves want to exploit

What is
Cyber Liability

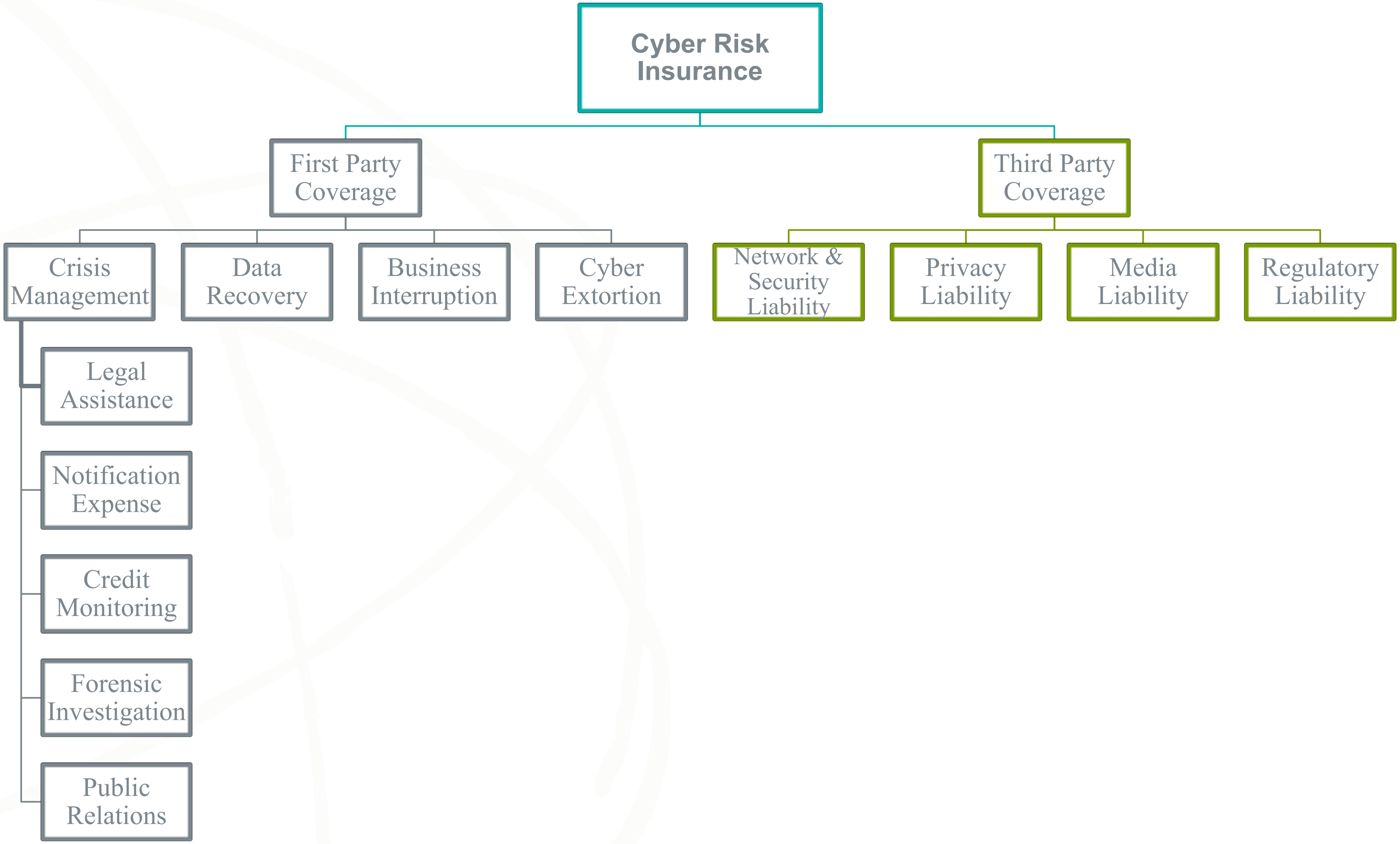
What is Cyber Risk Insurance?

Insurance coverage designed to protect a business or public entity from:

- Liability associated with:
    - Unauthorized release of confidential information
    - Violation of a person’s rights to privacy
    - Personal injury in an electronic/social media environment
    - Intellectual property infringement
    - Violations of state or federal privacy laws
- Self-incurred expenses incurred to make the above problems go away

Cyber Coverage Explained

First & Third Party



- Cyber Risk Insurance
  - First Party Coverage
    - Crisis Management
      - Legal Assistance
      - Notification Expense
      - Credit Monitoring
      - Forensic Investigation
      - Public Relations
    - Data Recovery
    - Business Interruption
    - Cyber Extortion
  - Third Party Coverage
    - Network & Security Liability
    - Privacy Liability
    - Media Liability
    - Regulatory Liability

Current Claims in the Pubic Entity Sector

- Real Events
- Recent Events
- Lessons Learned

Claim # 1

Type of Entity:	State Housing Authority
Type of Event:	Ransomware
Coverage Triggered:	Privacy & Security / Data Breach & Crisis Mgmt
Payout:	$250,000

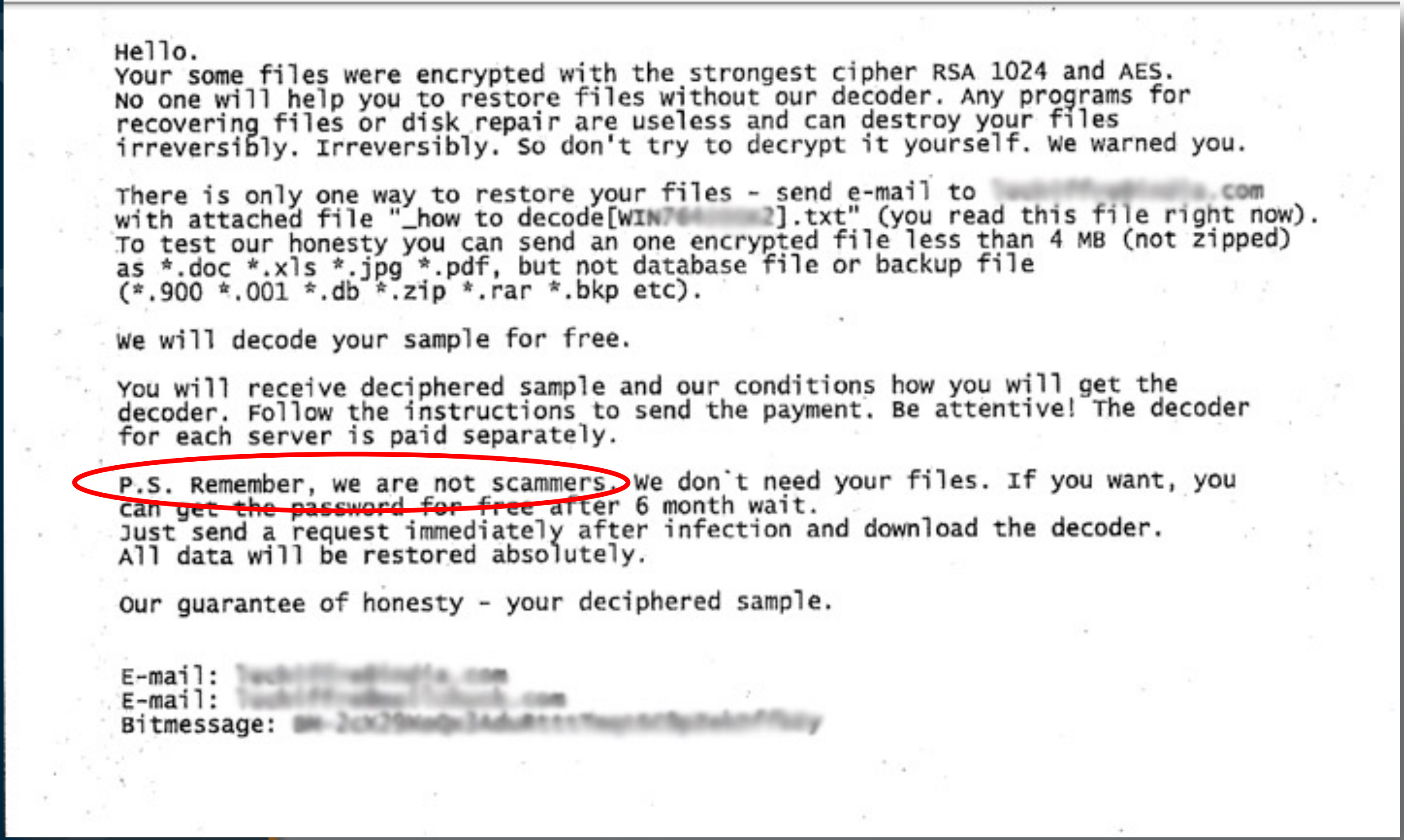
- Overview
  - Contacted outsourced IT provider
  - Wiped critical data/evidence, hindering response
  - Forensics engaged
  - Notification of 6,893 individuals, credit monitoring, public relations.

Claim # 2

- Type of Entity: Board of Education
- Type of Event: Ransomware
- Coverage Triggered: Cyber Extortion
- Anticipated Payout: > $25,000

- Overview
  - Employee opened email containing malware
  - Multiple computers and network drive affected
  - Legal counsel engaged
  - IT forensics
  - No data exfiltration

Ransomware



Hello.
Your some files were encrypted with the strongest cipher RSA 1024 and AES.
No one will help you to restore files without our decoder. Any programs for recovering files or disk repair are useless and can destroy your files irreversibly. Irreversibly. So don't try to decrypt it yourself. We warned you.

There is only one way to restore your files - send e-mail to [redacted] with attached file "_how to decode[WIN[redacted]2].txt" (you read this file right now).
To test our honesty you can send an one encrypted file less than 4 MB (not zipped) as *.doc *.xls *.jpg *.pdf, but not database file or backup file (*.900 *.001 *.db *.zip *.rar *.bkp etc).

We will decode your sample for free.

You will receive deciphered sample and our conditions how you will get the decoder. Follow the instructions to send the payment. Be attentive! The decoder for each server is paid separately.

P.S. Remember, we are not scammers. We don`t need your files. If you want, you can get the password for free after 6 month wait.
Just send a request immediately after infection and download the decoder.
All data will be restored absolutely.

Our guarantee of honesty - your deciphered sample.

E-mail: [redacted]
E-mail: [redacted]
Bitmessage: [redacted]

Source: RPS Technology & Cyber Client Claim received 8/16/16

Claim # 3

- Type of Entity: County Government
- Type of Event: Virus Encryption
- Coverage Triggered: Data Breach & Crisis Mgmt
- Anticipated Payout: TBD

- Overview
  - County servers shut down, Thanksgiving holiday
  - 911 center included
  - 42 servers – Mamba variant – full-disk encryption
  - Working with law enforcement, IT forensics
  - Determining next steps, including data exfiltration
  - Developing

Claim # 4

• Type of Entity:	Design Svcs Company
• Type of Event:	Ransomware
• Coverage Triggered:	Cyber Extortion
• Anticipated Payout:	$300,000

- Overview
  - Ransomware attack on insured's servers and backup servers.
  - Encryption made restoration from backup impossible
  - Bitcoin ransom
  - Extensive monitoring
  - No data exfiltration
  - Legal, forensics

Claim # 5

Type of Entity:	School District
Type of Event:	DDOS Attack
Coverage Triggered:	Privacy & Security / Data Breach & Crisis Mgmt
Anticipated Payout:	TBD

- Overview
  - Disruptions in internet service
  - Perpetuated by a student
  - IT forensics, legal and law enforcement engaged
  - Developing

Claim # 6

Type of Entity:	School District
Type of Event:	Unauthorized Access
Coverage Triggered:	Privacy & Security / Data Breach & Crisis Mgmt
Payout:	$80,000

- Overview
  - Student gained access to grades and other personal information on > 3,000 fellow students

Breach Prevention

- **Preventing Data Breach Through Common Sense Application**

Mitigating Information Risk in Your Agency

- Electronic Threats
  - Recognize the signs – computer performance
- Phishing – Beware!
  - Recognizing scams in email (source, content)
  - Examine URL’s
  - Be cautious about “Friend Requests” – personal & work separate
  - Do not “reply” – create new email
  - Do not open or download attachments from unknown sources

Mitigating Information Risk in Your Agency

- Password Guidelines
  - Strong passwords
  - Change frequently
  - Set screensavers to unlock with passwords
  - Do not share
- Electronic Safeguards
  - Security software
  - Securing your computer

Mitigating Information Risk in Your Agency

- Electronic Communications
  - Encryption
  - Beware of hyperlinks
  - Know your sender
  - Do not click “reply”
  - Verify source before downloading content
  - Never assume info is public knowledge – do not post to social media
- Physical Security
  - Beware of wandering eyes
  - Unauthorized physical access
  - Eavesdropping – not limited to electronic info
  - Mobile devices
  - Backup data off-site – segregated from network

Mitigating Information Risk in Your Agency

- Securing Office Areas & Resources
  - Desk, files, etc.
  - Retrieval of sensitive info
  - Disposal of sensitive info
- Safe Remote & Mobile Computing
  - Smart phones – turn off wireless when not in use
  - Flash drives - encrypt
- Protecting Info on Mobile Devices
  - Storing data on phones
  - Non-approved apps
  - Passwords/hints

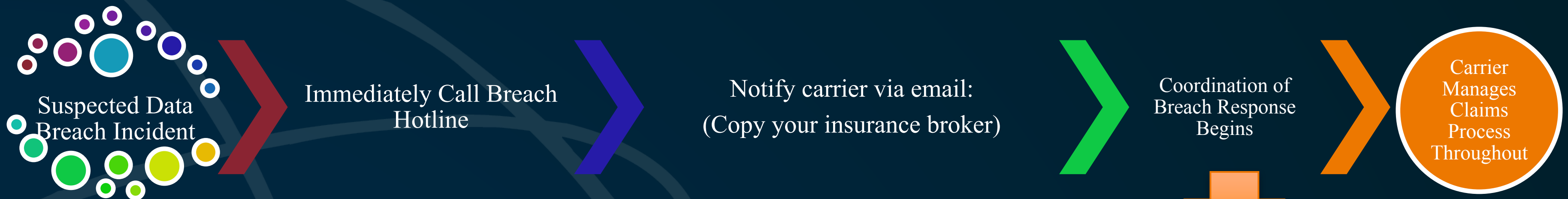
Mitigating Information Risk in Your Agency

- Safe Computing Away from the Office
  - Public transit
  - Home
  - Public places
  - Airports
  - Hotels
  - Do not email sensitive student info to your unsecured home email address for convenience

Incident Reporting

Breach Response

Expert Resources are Ready to Assist



Suspected Data Breach Incident

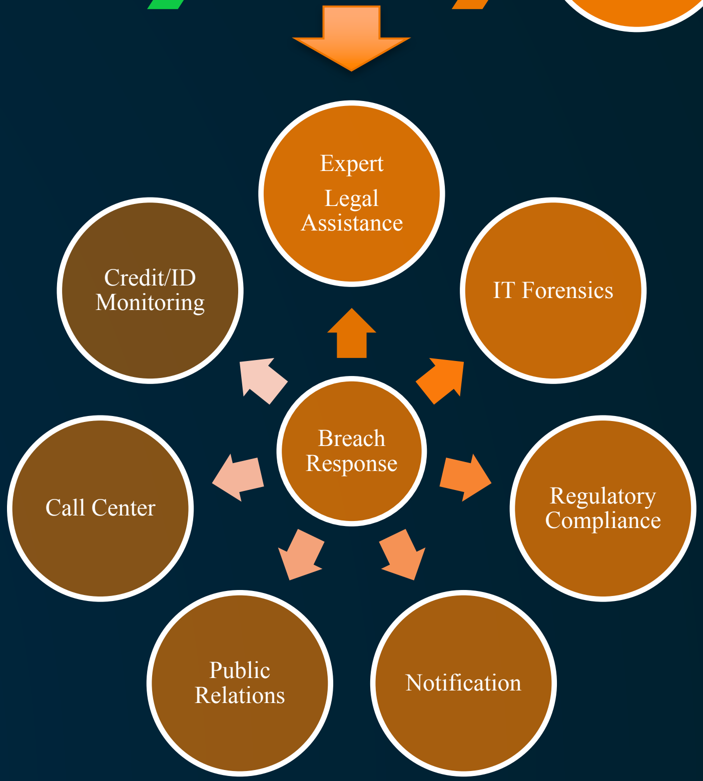
Immediately Call Breach Hotline

Notify carrier via email:

(Copy your insurance broker)

Coordination of Breach Response Begins

Carrier Manages Claims Process Throughout



Breach Response

Expert Legal Assistance

IT Forensics

Regulatory Compliance

Notification

Public Relations

Call Center

Credit/ID Monitoring

Goals:

- Ensure compliance
- Mitigate potential damage:
  - Financial
  - Operational
  - Reputational

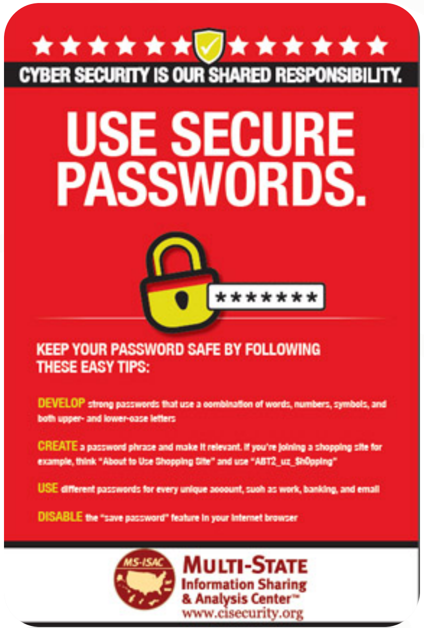
Do’s & Don’ts of Incident Reporting

- DO report any suspected privacy/information security incidents to your IT department/manager immediately – even if you are unsure
- DO prepare a brief description of the incident, timeline, key personnel
- DO call the insurance carrier Data Breach Hotline (if you have coverage)

- DO NOT attempt to handle the matter yourself
- DO NOT do anything to jeopardize the digital footprint of the incident
- DO NOT engage legal or forensics experts without first calling the insurance carrier Data Breach Hotline

Employee Awareness & Education

- The basics of cyber hygiene must get to the front line employees



CYBER SECURITY IS OUR SHARED RESPONSIBILITY.

USE SECURE PASSWORDS.

KEEP YOUR PASSWORD SAFE BY FOLLOWING THESE EASY TIPS:

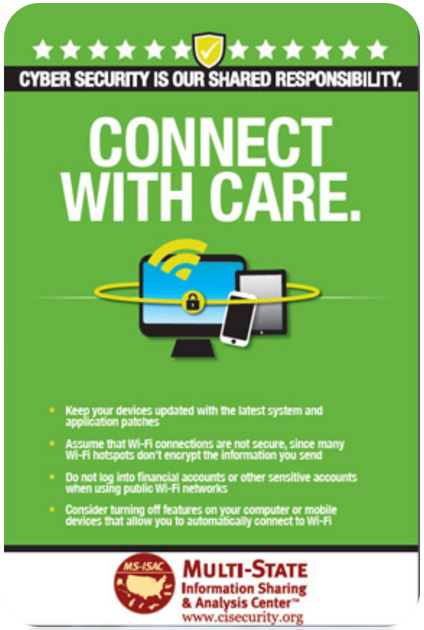
DEVELOP strong passwords that use a combination of words, numbers, symbols, and both upper- and lower-case letters

CREATE a password phrase and make it relevant. If you're joining a shopping site for example, think "About to Use Shopping Site" and use "ABT2_uz_$h0pping"

USE different passwords for every unique account, such as work, banking, and email

DISABLE the "save password" feature in your Internet browser

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
www.cisecurity.org

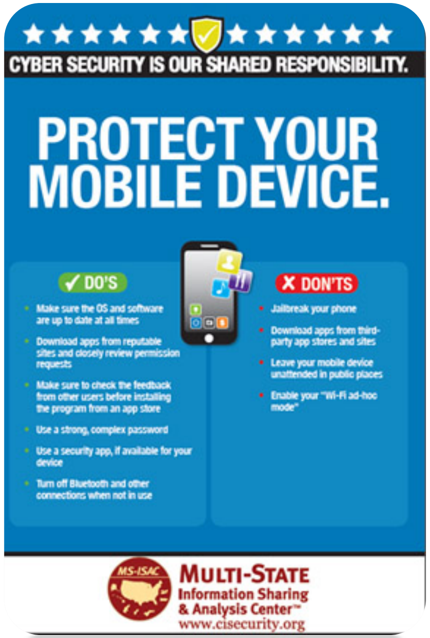


CYBER SECURITY IS OUR SHARED RESPONSIBILITY.

CONNECT WITH CARE.

- Keep your devices updated with the latest system and application patches
- Assume that Wi-Fi connections are not secure, since many Wi-Fi hotspots don't encrypt the information you send
- Do not log into financial accounts or other sensitive accounts when using public Wi-Fi networks
- Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
www.cisecurity.org



CYBER SECURITY IS OUR SHARED RESPONSIBILITY.

PROTECT YOUR MOBILE DEVICE.

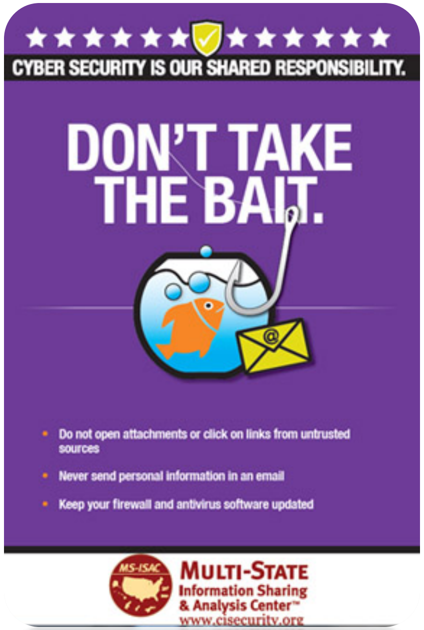
✓ DO'S

- Make sure the OS and software are up to date at all times
- Download apps from reputable sites and closely review permission requests
- Make sure to check the feedback from other users before installing the program from an app store
- Use a strong, complex password
- Use a security app, if available for your device
- Turn off Bluetooth and other connections when not in use

✗ DON'TS

- Jailbreak your phone
- Download apps from third-party app stores and sites
- Leave your mobile device unattended in public places
- Enable your "Wi-Fi ad-hoc mode"

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
www.cisecurity.org



CYBER SECURITY IS OUR SHARED RESPONSIBILITY.

DON'T TAKE THE BAIT.

- Do not open attachments or click on links from untrusted sources
- Never send personal information in an email
- Keep your firewall and antivirus software updated

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™
www.cisecurity.org

Questions

Thank You!