HUB

Cyber Exposure and Liability

Alaska Municipal Management Association
November 13, 2017

Objectives

- Define Cyber Liability
- Data Risks
- Hackers and Viruses
- Phishing and Spoofing
- Ransomware
- Preventing Hacking
- Notification Requirements
- Cyber Security Policy
- Available Coverages
- Cyber Rick Management Services

What is Cyber Liability

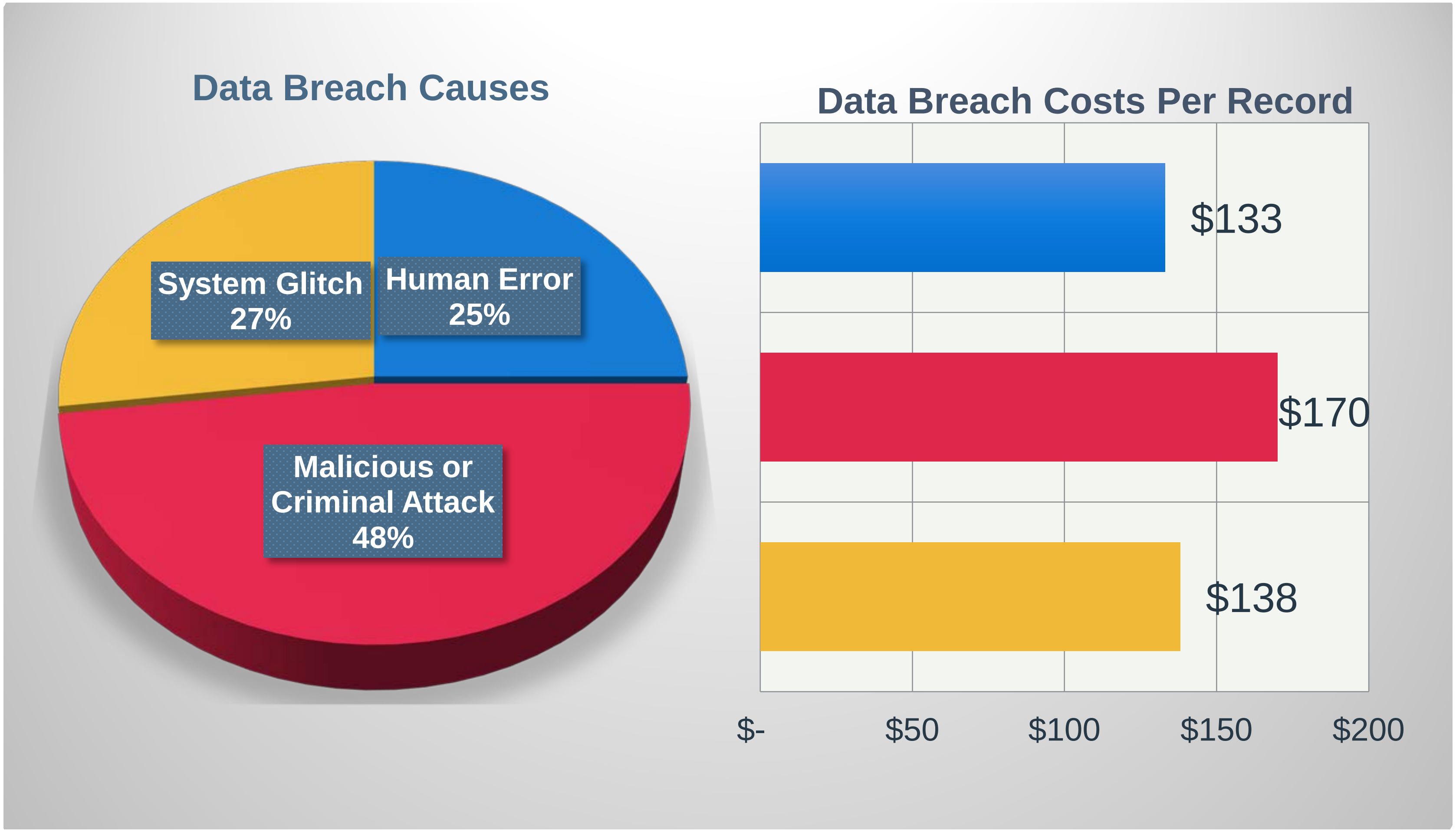
- Exposures arising from the use of computers, networks, and the internet
- Liability associated with the compromise of confidential and personal information

Data Governance & Data Risks

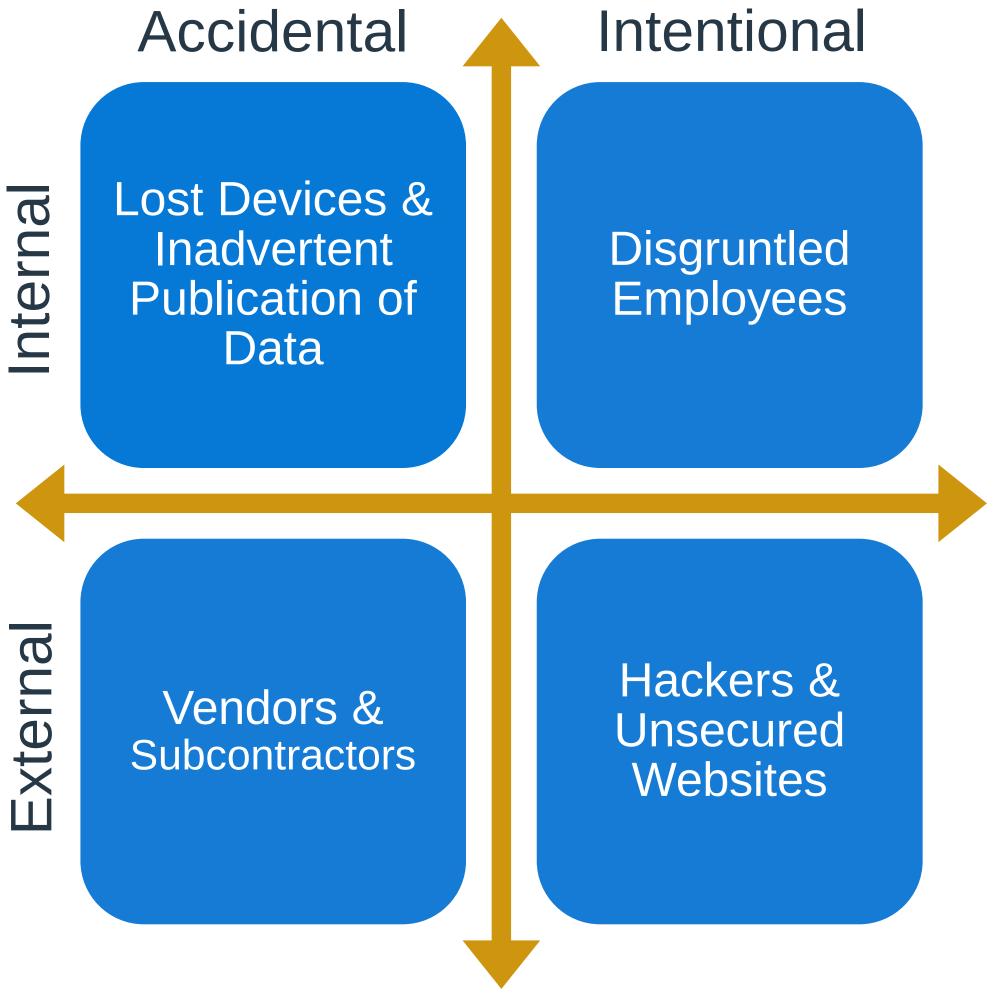
Owning data creates legal duties

- What data do you collect and why ?
- Where is it ?
- How well is it protected ?
- Who can access it ?
- When do you purge it ?
- How do you purge it ?

Causes & Costs of Data Breaches



How Do Incidents Occur ?



Accidental

Intentional

Internal

External

Lost Devices & Inadvertent Publication of Data

Disgruntled Employees

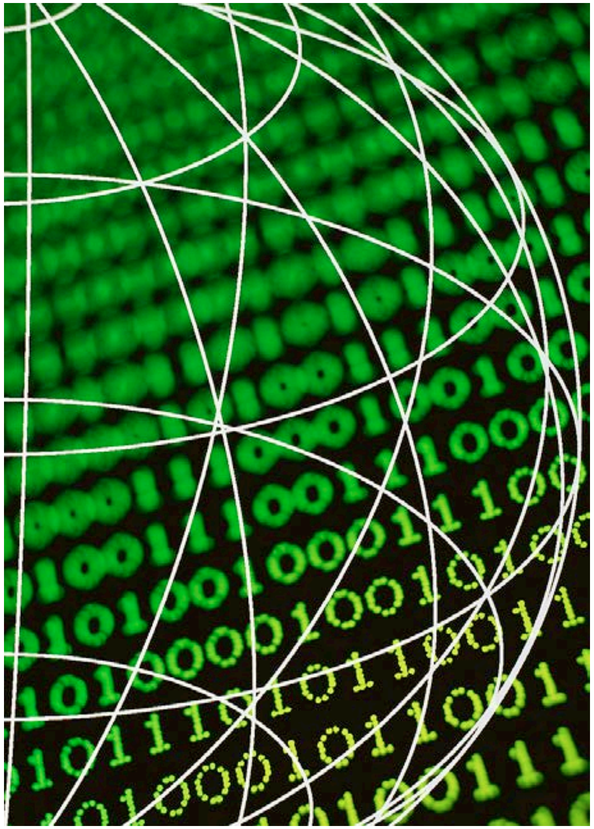
Vendors & Subcontractors

Hackers & Unsecured Websites

Source: Navigant Consulting

Types of Data

- PII – Personally Identifiable Information
  - *i.e.*, Name in combination with social security number, driver’s license number, bank account information, credit card information, username and password.
- PHI – Protected Health Information
  - Information relating to provision of healthcare that can be used to identify an individual
- PCI – Payment Card Industry Information
  - Cardholder data
- Intellectual Property / Trade Secrets



Hacking

- Unauthorized use of or access to computers or networks
- Hackers can control your computer and network
- Hackers can:
  - Access files
  - Add, change, or delete information

Malware

- Common types of Malware
  - Computer Viruses
  - Worms
  - Trojan Horses
  - Bots

Malware

Computer Viruses

- Can corrupt or delete data
- Spread through email to other computers
- Return information to the source

The Melissa Virus

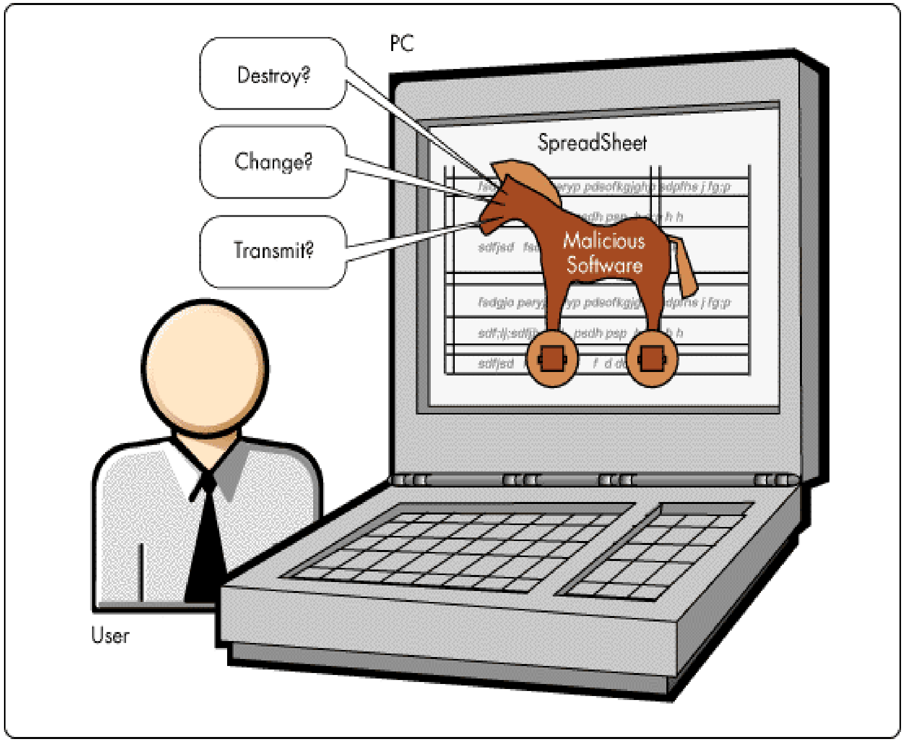
- When opened it sent the infected attachment to the first 50 contacts
- Caused Intel and Microsoft to shut down their email servers

Malware

- Worms
  - Copies itself and spreads to other computers
  - Use computer processing time and bandwidth
  - Can delete files on host system
- MyDoom Worm of 2004
  - Worm would duplicate and send itself to email address in the address book
  - Millions were affected
  - Damage was over $22 billion

Malware

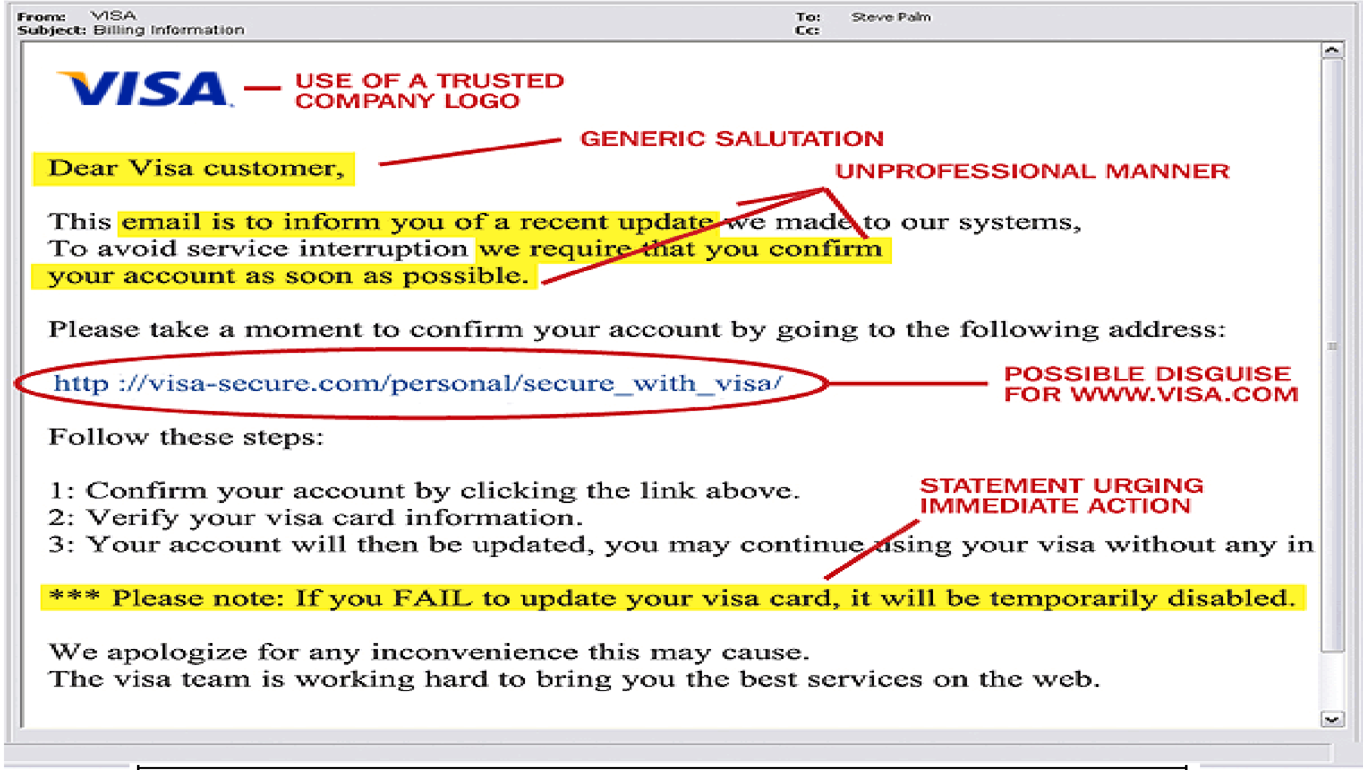
- Trojan Horses
  - Usually attached to programs that seem to have a legitimate purpose
  - Allow attacker to steal/modify data
  - Give capability to screen watching and keylogging



Phishing and Spoofing

- E-mails, websites, or text messages trying to steal money or information
- Falsely claiming to be a legitimate business, website, or group
- How to identify:
  - Misspellings and grammatical errors
  - Threats
  - Peculiar hyperlinks and attachments

Phishing and Spoofing



From: VISA
Subject: Billing Information
To: Steve Palm
Cc:

VISA

Dear Visa customer,

This email is to inform you of a recent update we made to our systems,
To avoid service interruption we require that you confirm
your account as soon as possible.

Please take a moment to confirm your account by going to the following address:

http ://visa-secure.com/personal/secure_with_visa/

Follow these steps:

1: Confirm your account by clicking the link above.
2: Verify your visa card information.
3: Your account will then be updated, you may continue using your visa without any in

*** Please note: If you FAIL to update your visa card, it will be temporarily disabled.

We apologize for any inconvenience this may cause.
The visa team is working hard to bring you the best services on the web.

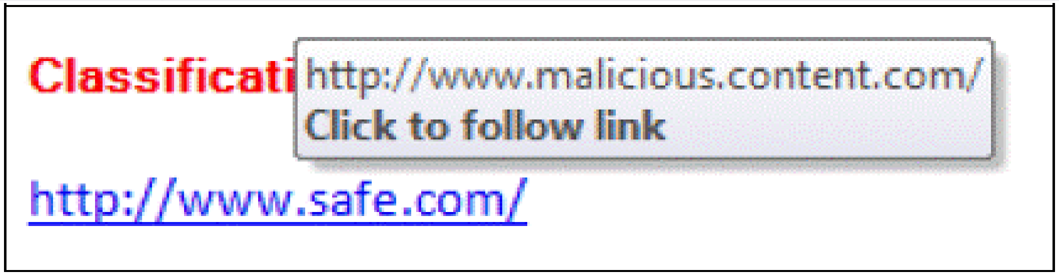
USE OF A TRUSTED COMPANY LOGO

GENERIC SALUTATION

UNPROFESSIONAL MANNER

POSSIBLE DISGUISE FOR WWW.VISA.COM

STATEMENT URGING IMMEDIATE ACTION



Classificati

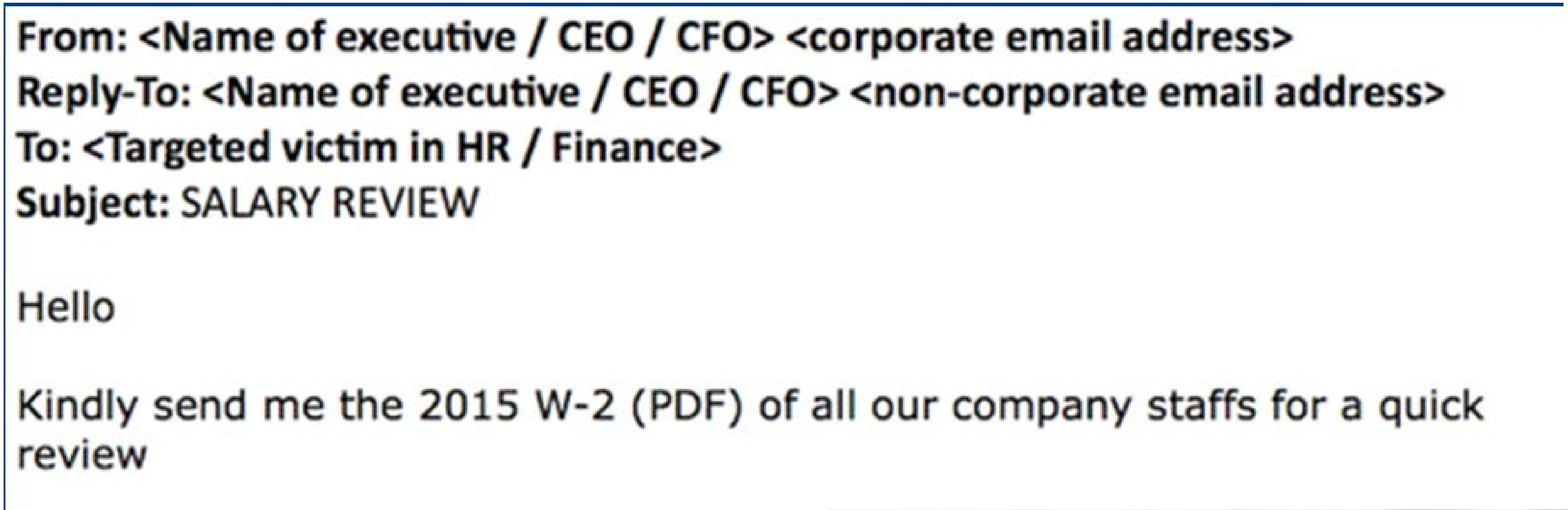
http://www.malicious.content.com/
Click to follow link

http://www.safe.com/

Phishing and Spoofing

- A ring of middle school students were able to gain access to and control of more than 300 computers by phishing for teacher administrative codes. At least 18 students were involved. The breach happened when students used software to imitate a legitimate software update on their computers. The students then asked teachers to enter administrative account information so that they could complete the software updates or installations. The phony software then stored teacher credentials. The students were then able to control 300 laptops belonging to other students by using the administrative credentials. The school believes that servers and sensitive information were not exposed. The breach occurred around Friday, April 26 and was discovered on Monday, April 29 when students noticed that other students appeared to be controlling student laptops remotely and reported the issue.

Phishing Attacks



From: <Name of executive / CEO / CFO> <corporate email address>
Reply-To: <Name of executive / CEO / CFO> <non-corporate email address>
To: <Targeted victim in HR / Finance>
Subject: SALARY REVIEW

Hello

Kindly send me the 2015 W-2 (PDF) of all our company staffs for a quick review

Thanks

Form W-2 Wage and Tax Statement
Copy B To Be Filed With Employee's FEDERAL
31a and 32 - 3
line 36 from
Act, and Pap

Ransomware: The Latest Threat

- Form of malware transmitted through links and attachments
- 60% malware payloads were ransomware Q1 2017
- 70% of companies targeted have been infected
- Ransom demands –Currently average $1000
- FBI Reports cost $1B in 2016, projected $5B for 2017
- To pay or not to pay? What type of data? Can we live without it?
- Is there a backup?
- Costs of business interruption?
- There are no guarantees

If A Ransomware Attack Happens To You

- Immediately disconnect affected computer from network
- Don’t communicate with the hacker – refer to internal IT security
- Don’t try to alter systems or investigate on your own

How to prevent Hacking

- Perform software updates
- Install firewalls
- Continually update passwords
- Install anti-virus software
- Install updates

.

Strong Password Security

- Make your passwords long
- Include letters, punctuation, symbols, and numbers
- Change your passwords often
- Don’t use the same password for everything
- Never share passwords
- Don’t write your passwords down

Top 10 common passwords in 2016

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball

Create a Cyber Security Policy

- Require regular password changes
- Enforce password requirements
- Limit system access to those who need it
- Remove access when it is no longer needed
- TRAIN EMPLOYEES

Review

- Protect yourself from hackers and viruses
- Be aware of Phishing and Spoofing
- Keep your portable devices secured
- Practice and maintain good password security
- Requirements for outside vendors
- Have a good cyber security policy

The Update Protocol

- **U**pdate Frequently
- **P**asswords
- **D**ownload
- **A**dmin
- **T**urn-Off
- **E**ncrypt

What Happens if a Breach Occurs

Notification Requirements

- A.S. 45.48.010
  - Disclose the breach to all affected residents
  - Must notify in the “most expeditious time possible and without unreasonable delay.”
  - Notice may be delayed if a law enforcement agency finds it would interfere with a criminal investigation
- Failure to comply
  - $500 for each affected state resident, up to $50,000

Notification Requirements

- Notification methods
  - Written document sent to resident’s most recent address on file
  - Electronically, if that is the primary method of communication
  - Under special circumstances in lieu of written communication you may:
    - Provide e-mail notification
    - Post disclosure conspicuously on your website
    - Notify major statewide media

Available Coverage Overview

- **Network Security Liability:** Liability to a 3rd party as a result of a failure of company's network security to protect against destruction, deletion or corruption of a 3rd party’s electronic data, denial of service attacks against Internet sites or computers; or transmission of viruses to third party computers and systems.
- **Privacy Liability:** Liability to a 3rd party as a result of company's failure to properly handle, manage, store or otherwise control personally identifiable information, corporate information identified a confidential and protected under a nondisclosure agreement and unintentional violation of privacy regulations.
- **Regulatory:** Defense expenses and civil fines or penalties paid to a governmental entity in connection with an investigative demand or civil proceeding regarding actual or alleged violation of privacy laws
- **Identity Theft Response Fund:** Expenses to comply with privacy regulations, such as communication to and credit monitoring services for affected customers. This also includes expenses incurred in retaining a public relations firm for the purpose of protecting/restoring company's reputation as a result of the actual or alleged violation of privacy regulations.

Available Coverage Overview

- **Network Business Interruption:** reimbursement of the company's own loss of income or extra expense resulting from an interruption or suspension of its systems due to a failure of network security to prevent a security breach.
- **Data Asset Protection:** recovery of the company's costs and expenses incurred to restore, recreate or regain access to any software or electronic data from back-ups or from originals or to gather, assemble and recreate such software or electronic data from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion or damage.
- **Cyber Extortion:** ransom or investigative expenses associated a threat directed at the company to release, divulge, disseminate, destroy, steal, or use the confidential information taken from the Insured, introduce malicious code into the company's computer system; corrupt, damage or destroy company's computer system, or restrict or hinder access to the company's computer system.

Cyber Risk Management Services

Hub Risk Services provides the full range of expert consulting to identify risks, reduce exposure to loss and manage claims issues. Risk Services works closely with clients to provide cyber risk management for greater cyber resilience.

Our team can assist with identification, compliance, mitigation, detection and response from cyber threats, attacks and breaches. These services minimize technology failures, customer harm, reputational damage and financial loss.

- Cyber Incident Response Planning
- IT Security Program Assessment
- Cyber Risk Assessments
- Cyber Activity Risk Assessment
- Cyber Incident Response Exercises
- HIPAA Compliance Support
- IT Third Party Risk Management
- Instructor or Webinar Led Cyber Training
- IT Security Policies
- Audits

Questions?

Thank you.

HUB International Northeast Limited
35681 Kenai Spur Hwy
Soldotna AK 99669

Doug Brown
Senior Vice President
+1 (907) 262-4425 Office
doug.brown@hubinternational.com