# Data Security Best Practices

We can show you more.®

TECHNOLOGY

**PRESENTED BY: Nick Graf**

**November 12, 2015**

# Disclaimer



The information, examples and suggestions presented in this material have been developed from sources believed to be reliable, but they should not be construed as legal or other professional advice. CNA accepts no responsibility for the accuracy or completeness of this material and recommends the consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. This material is for illustrative purposes and is not intended to constitute a contract. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice.

Any references to non-CNA Web sites are provided solely for convenience and CNA disclaims any responsibility with respect thereto.



# Agenda



- Trends
- Update
- Emerging Cyber risk
- Best in Class Controls
  - Separating the Good from the Bad
- Data Security Strategy
- Risk Management
- Cyber Insurance Coverage

# Trends



- Cyber Events of 2014[1]
  - 79,790 confirmed security incidents
  - 2,122 confirmed data breaches

- Security Incident = Any event that compromises the confidentiality, integrity, or availability or an information asset.

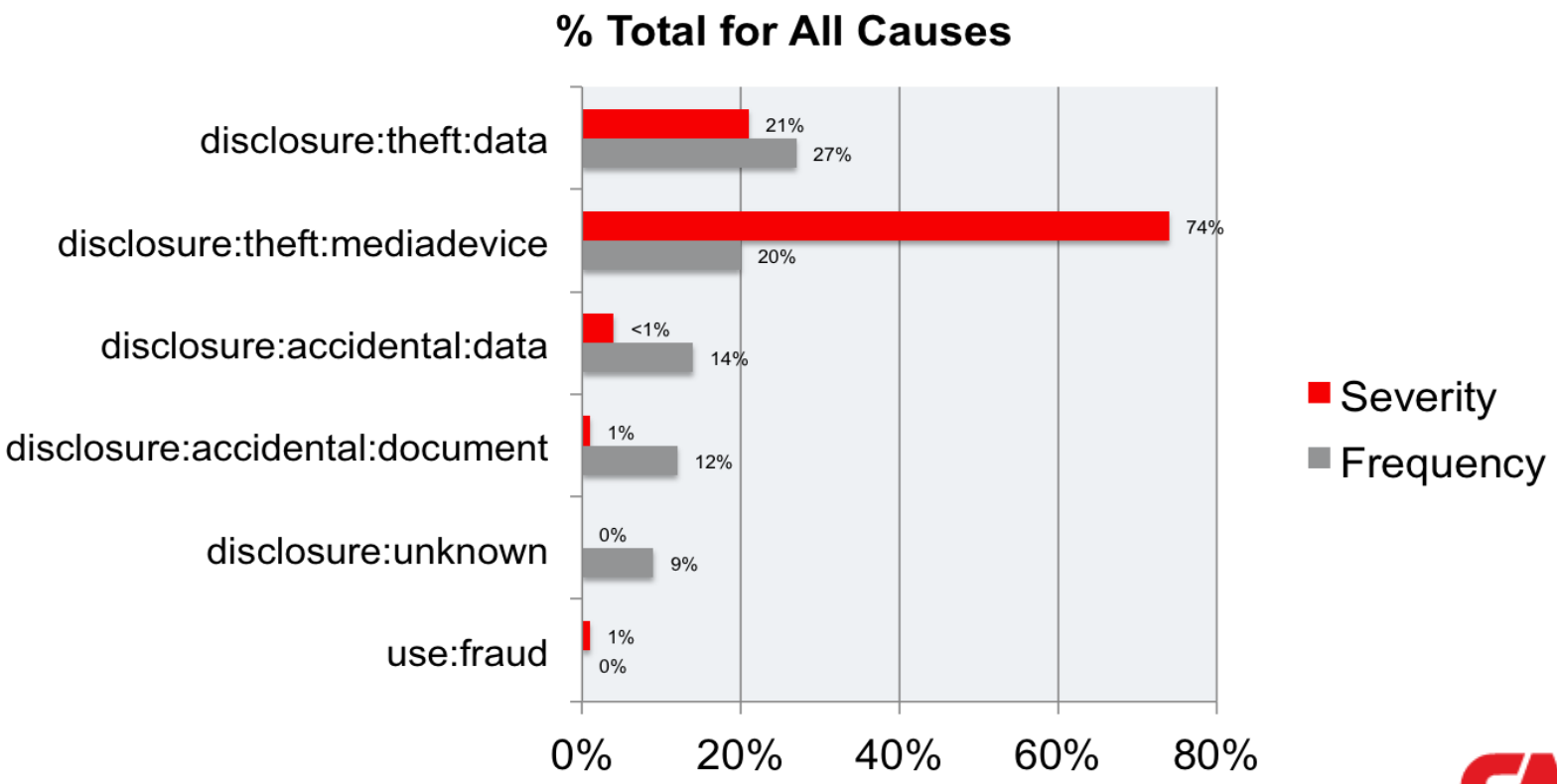
- Data breach = An incident that resulted in confirmed disclosure to an unauthorized party.

1 : *Verizon 2015 Breach Investigations Report. Conducted by Verizon. Publication April 2015*

# Causes



Top causes of Data Breaches – CNA Claim Data (2003-2013)



# Trends



- Top Threats: Phishing
  - 50% of recipients open email and click on link within the first hour
  - Median time-to-first-click: one minute, 22 seconds
  - Campaign of 10 emails have a greater than 90% chance of success

- How to Minimize Phishing
  - Better email filtering
  - Improved detection capabilities
  - Thorough security awareness program

*Statistical data reference: see Verizon 2015 Data Breach Report, page 13*

# Update



- Top Threats: Vulnerabilities
  - 99.9% of vulnerabilities compromised more than a year after first discovered
  - 10 vulnerabilities represent 97% of exploits in 2014
  - More than 7 million exploited vulnerabilities

- How to Minimize Vulnerabilities
  - Patch
  - Remove unnecessary services (web, database, remote administration)
    - Part of the larger “hardening” efforts: http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
  - Remove unnecessary information: hiding software version and OS identify: http://www.tecmint.com/apache-security-tips/

CNA

# Emerging areas of risk



- Embedded Devices
  - Heating and Ventilation
  - Medical Devices
  - Personal Fitness Trackers
- Automobiles
  - Current vs future
- Airplanes
- Commonalities?

- Why do “they” do it?
  - Competitive advantage
  - Skip Research and Development
  - Espionage

# Who are the attackers?



- Where do they “lurk”?
  - Deep web
  - Underground market places
  - Utilizing TOR
- Who are they?
  - All walks of life
  - Disgruntled unemployed “coders”
  - Teenagers sitting in mom’s basement
  - Nation state sponsored paramilitary groups
- How do they do it?
  - What you see in TV and the Movies isn’t real
  - Some traditional hacking
  - Social engineering with increasing frequency

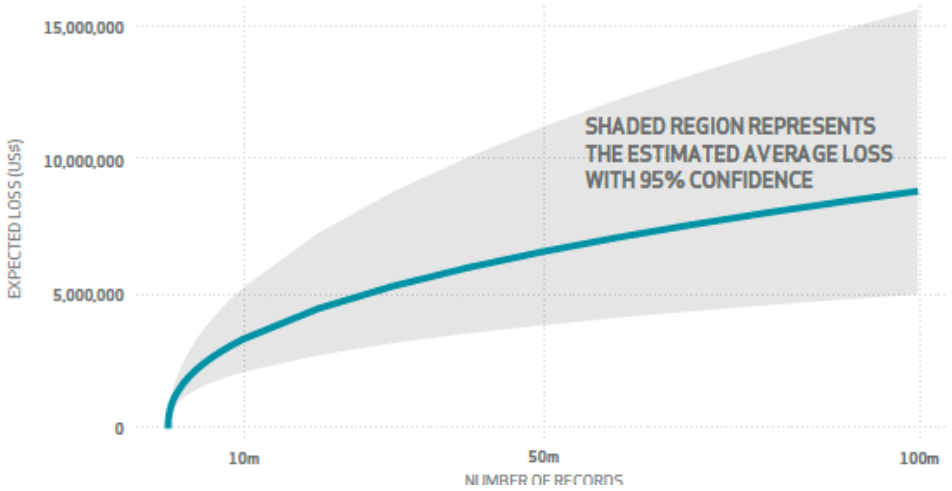
CNA

# Cost of an incident



- $154[1] vs. $0.58[4]  Who's right?
- Many factors go into the cost
- "The forecasted average loss for a breach of 1,000 records is between $52,000 and $87,000"[2]
- Forensics – Paid like lawyers

3




1 ,2 & 3: *Verizon 2015 Breach Investigations Report. Conducted by Verizon. Publication April 2015*
4: *2015 Annual Study: U.S. Cost of a Data Breach*. Sponsored by IBM, Independent Research by Ponemon Institute, LLC. Publication May 2015

CNA

# Best in Class Controls



- Full disk encryption on all laptops, desktops, mobile devices, and external storage
- Segmentation of network – example: Target
- Controls extending to embedded devices
- Documented and tested DR/BC and Incident Response plans
- Formal Data Retention Policy – including secure deletion of data
- Two Factor authentication
- Physical Security
- Robust Cloud/Vendor management system
- Security awareness training
- Understanding the additional controls necessary for PCI and HIPAA
- Conducting annual penetration tests, and remediating issues

CNA

# Separating the Good from the Bad



- **Varies depending on the company size**
- Having a disaster recovery plan that it 5 years old and has never been tested
- Unencrypted laptops – “But we have a policy!”
- Unencrypted credit card data
- “We retain everything forever” as a retention policy
- “But we’re PCI compliant”
- “I’ve outsourced that function so we don’t need to worry about it”
- “That’s on our roadmap for 2016…”
- Who is the most senior person responsible for Information Security?

CNA

# Data Security Strategy



- Don’t reinvent the wheel
  - NIST Cyber Security Framework: http://www.nist.gov/cyberframework/
  - NIST guide to server security: http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
  - NIST guide to incident response: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
  - NIST guide to DR and BC planning: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
  - Classify data and identify it’s location

CNA

# Risk Management



- Acceptance
  - Active versus Passive
- Avoidance
  - Location of a datacenter
- Mitigation
  - Compensating controls
- Transference
  - Insurance

# What is and isn’t covered?



- Type of Coverage
  - Errors and Omissions
  - Media
  - Network Security
  - Privacy
- First Party vs. Third Party
- Sub-Limits and Deductibles
- Not covered:
  - Future revenue
  - Business Reputation
  - Improvements
  - Intellectual Property

CNA

# Closing thoughts



- Think outside the box
  - Other internet connected devices may present risk to your organization
- Security awareness training of employees is crucial
- Leverage tools from NIST (and others) to create a mature security program
- Have a thorough understanding of what is and isn't' covered by insurance

# Thanks!



Questions?  Comments?