



WTA Spring Meeting 2017: Cybersecurity Discussion



Erin Fitzgerald

efitzgerald@bennetlaw.com



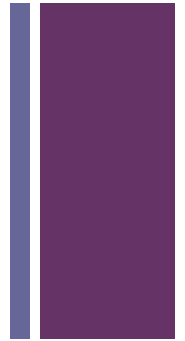
+



Cyber Threat Basics



Cyber Threat Basics



- **Why does cybersecurity matter?**
 - 170 million malware incidents affected 20,000 organizations in just one year.
 - Attackers took minutes or less to compromise systems in 94% of cases.
 - Attacks spread from the first victim to others within 24 hours 75% of the time.
 - Attacks cost American companies \$246 for each compromised record.
- **...And these are just the attacks that we know about.**

+ Who Is Attacking Us...And Why?

■ Individuals and Criminal Groups

- Sale of personally identifiable information (PII), intellectual property, financial data and almost any information with economic value.
- A black market has emerged around the acquisition of and sale of this information.

**IT'S
ABOUT
THE
MONEY!**

Information	Price/Record
Fresh credit card data	\$20-25
Stale credit card data	\$2-7
Medical record	\$50
Hijacked email account	\$10-100
Bank account credentials	\$10-1000

Example pricelist for stolen information

Oracle, Securing Information in the New Digital Economy, 2015

+ **One More Time: It's About Money!**

- The hacker economy is one of the most lucrative in the black market.

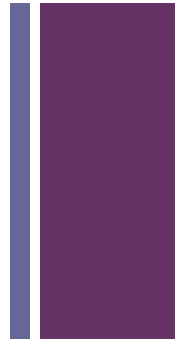
- **Stolen Smartphones: \$30 Billion**

- **Stolen Vehicles: \$56 Billion**

- **Cocaine Drug Trade: \$85 Billion**

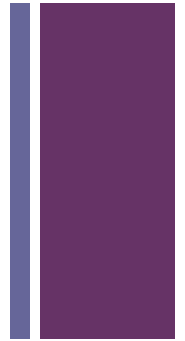
- **Stolen Credit Cards: \$114 Billion**

- **Total Global Cybercrime: \$288 Billion**



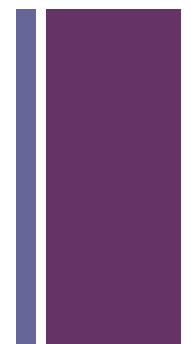


How Does This Happen?



- **Target:** In December 2013, Target confirmed that criminals had infiltrated its system, installed malware on its point-of-sale network, and potentially gained access to guest payment and credit card data. More than 100 million people could have been affected.
- **OMB:** Officials believe that this 2015 hack by the Chinese government compromised sensitive personal information, including Social Security numbers, of roughly 21.5 million people from both inside and outside the government.
- **Veterans Affairs:** A 2006 laptop theft exposed unencrypted information for 26.5 million people.

+ What Does the Cyber Threat Mean to Rural Telecom Operators?



- **No entity is too small for a cyber attack.** In fact, cyber criminals view individuals and small organizations as easy targets due to the belief that they have limited defenses and cybersecurity resources.
- **Theft of subscriber information.** Personally Identifiable Information (PII), Personal Credit Card Information (PCI).
- **Erosion of business reputation.**
- **Impact on network performance.**
- **Costly.** Breaches are detrimental to an entity's bottom line.
- **A prerequisite to enter new business?** Your customers may already be asking you what kind cybersecurity and procedures you have in place.
- The question is not whether your firewalls, anti-virus, and anti-malware software will be breached. The question is when.



+ **FTC Enforcement Authority
Over Data Security**



+ FTC Authority Over Data Security

- FTC Act prohibits “unfair or deceptive acts or practices, in or affecting commerce.”
- **Enforcement, rather than regulatory, authority.**
 - FTC investigates business practices on a case-by-case basis instead of promulgating rules and regulations.
 - Investigation may result in the FTC filing suit in federal court.
- **FTC cases are almost always settled.**
 - Most information is never publicly released – known only to the FTC and the business being investigated.
- **Wyndham Hotels Case:** Hackers stole customers’ personal and financial information – resulting in over \$10.6 million dollars in fraudulent charges.
 - FTC filed suit, alleging that the failure to secure private data was an unfair practice, and that Wyndham’s privacy policy was deceptive.
 - Court of Appeals found that FTC has authority to regulate data security practices.

+ FTC Common Carrier Exemption

- **FTC Act exempts common carriers from the FTC's authority.**
 - FTC cannot bring enforcement actions against common carriers with respect to provision of common carrier services.
- **Historically, this exemption didn't include Internet service providers (ISPs).**
 - FCC's 2015 *Open Internet Order* changed this.
 - ISPs now telecommunications carriers subject to Title II common carrier regulation.
- **November 2015 – FTC and FCC Memo of Understanding**
 - “The agencies express their belief that the scope of the common carrier exemption does not preclude the FTC from addressing non-common carrier activities engaged in by common carriers.”
 - To be continued....

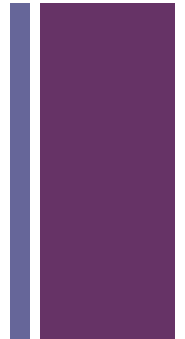


+ FCC Regulatory Authority
Under Section 222





FCC Statutory Authority



- **Communications Act, Section 222:**
 - “Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of...other telecommunication carriers, equipment manufacturers, and customers...”
- FCC historically interpreted Section 222 in the CPNI context.
 - CPNI includes technical/call information made available to carrier by the customer solely by virtue of the carrier-customer relationship.
- FCC expanded this interpretation in the TerraCom/YourTel Data Breach Notice of Apparent Liability (NAL).

+ 2014 TerraCom/YourTel Data Breach

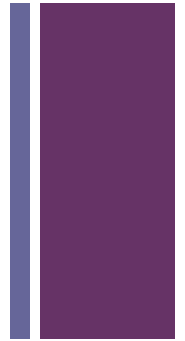
- TerraCom and YourTel are wireless resellers.
 - Designated as Lifeline-only ETCs.
 - Collected enrollee personal information.
- TerraCom and YourTel stored this information on servers connected to the Internet.
 - Information was not password protected or encrypted and could be accessed by anyone.
 - FCC investigated and brought enforcement action.
- FCC issued a NAL in October 2014 for \$10 million.
 - This was the FCC's first ever data security case and the largest privacy action in its 80-year history.
 - Case was settled for \$3.5 million.

+ 2014 TerraCom/YourTel Data Breach

- FCC interpreted Section 222 to include private information that customers have an interest in protecting from public exposure – not just CPNI.
- Carriers have a duty under Section 222 to protect customer proprietary information.
 - Duty is triggered when a carrier accepts confidential private information from a potential customer as part of the service enrollment process.
- FCC concluded that TerraCom and YourTel breached the duty because it stored that information on servers that were publicly accessible.
- **Take Away:** TerraCom and YourTel deserved to be fined. They did not even have the most basic protection in place – passwords.

+ 2015 Cox Communications Breach

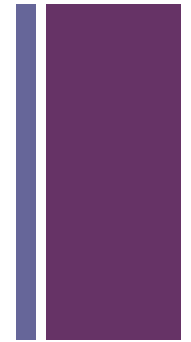
- Breach involved information from approximately **61** of Cox Communications' **6 million+** subscribers.
- Amateur hackers social-engineered Cox employees.
 - No technical failure involved.
 - No payment information accessed.
- Hackers posted information about **8** affected consumers on social media.
- Cox detected and halted the breach within days and worked with the FBI, who arrested the hacker.
- No evidence of consumer harm.
- But the settlement imposed a **\$595,000 fine** – nearly **\$10,000 per affected consumer** – and extensive compliance measures.
 - Serious **wake-up call** to companies subject to FCC jurisdiction.
 - FCC's action has been described as enforcement based on a **strict liability standard**.





Factors to Consider

- Enforcement actions related to data security violations will be driven by a number of factors:
 - Breach volume (*i.e.*, how *many* individuals affected, how *much* private information compromised, etc.);
 - Whether the entity at fault made a meaningful effort at appropriate security practices (*i.e.*, did it have breach prevention security measures in place);
 - Enforcement will be more likely for entities that are repeatedly compromised (especially if due to the same mistake);
 - Particular industries or businesses seen as having lax standards will be more likely to be subject to enforcement actions;
 - Enforcement agency may go after certain practices representative of a broader problem affecting many companies or industries (don't be a poster child).
 - FCC Enforcement Bureau activity level.



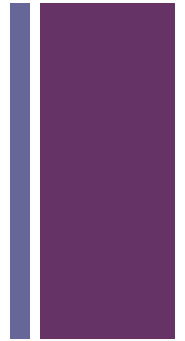
Broadband and Telecommunications Privacy Rules

+





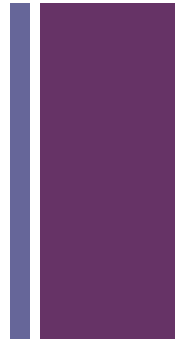
Background



- In the **2015 *Open Internet Order***, FCC reclassified broadband Internet access service (BIAS) from an information service to a telecommunications service.
 - BIAS now subject to Communications Act Title II.
 - Privacy rules released on Nov. 2, 2016. They are applicable to provision of all telecommunications services (including BIAS and VoIP).
 - Governs the use/protection of “customer proprietary information”
 - Individually identifiable Customer Proprietary Network Information (CPNI);
 - Personally identifiable information (PII); and
 - Content of communications
- Order contains requirements in the following areas:
 - **Customer Notice**
 - the types of information collected;
 - how and for what purposes the information is used/shared;
 - types of entities with which information is shared
 - **Securing customer consent before using certain types of PI**
 - **Data Security**
 - **Breach Notification**



Data Security Requirements



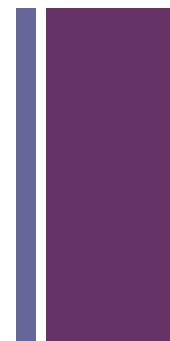
- Carriers must take reasonable measures to protect customer PI from unauthorized use, disclosure, or access.
 - A provider's practices must be appropriately calibrated to the: (1) nature and scope of its activities, (2) sensitivity of the data it collects, (3) size of the provider, and (4) technical feasibility.
 - A reasonability, rather than strict liability, standard.
 - No checklist.
- FCC has provided guidelines on steps that providers should consider in developing reasonable data security practices:
 - **Implement up-to-date/relevant industry best practices.**
 - NIST Cybersecurity Framework, 2015 FTC Security Guide, guidance on HIPAA and other statutory frameworks, CSRIC.
 - **Provide accountability and oversight of security practices.**
 - A written comprehensive data security program, designation of senior management official with personal responsibility for data security practices, employee and contractor training, third party data commitments.
 - **Implement robust customer authentication tools.**
 - Encourage stronger alternatives to customer-generated passwords or static security questions, notify customers of account changes and attempted changes, reassess.
 - **Other Practices.**
 - Properly dispose of data consistent with FTC best practices and the Consumer Privacy Bill of Rights; encrypt sensitive data; participate in lawful information sharing (CISA).

■ Effective date has been stayed pending Order on Reconsideration. © Bennet & Bennet, PLLC



Data Breach

Notification Requirements

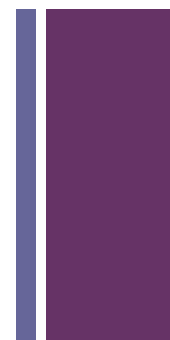


- Affected customers must be notified as soon as possible, but no later than 30 days after “reasonable determination” of a breach;
- In the event of a data breach affecting more than 5,000 customers, the FCC, FBI and the U.S. Secret Service must be notified within seven business days after reasonable determination of a breach;
- For data breaches affecting less than 5,000 customers, the FCC must be notified at the same time as customers;
- No notification necessary when a provider reasonably determines the breach will not cause harm to consumers.
 - Providers must take the investigative steps necessary to reach a reasonable determination that no such harm is reasonably likely. FCC established a rebuttable presumption that any breach involving sensitive customer PI presumptively poses a reasonable likelihood of customer harm and would therefore require customer notification.
 - FCC has expanded the definition of breach by adopting a harm-based trigger rather than a trigger based on intent and creates the obligation to report breaches that may harm consumers, regardless of the source or cause of the breach, or intent.
- Where the FCC’s rules are inconsistent with state laws, FCC rules will preempt those laws.



Creating a Cyber Risk Management Plan

+ Cyber Risk Management Plan



- **Technology: Consider engaging external/professional service providers to:**
 - Provide remote security monitoring management services.
 - Provide firewall, anti-virus, and network defense that adapts to the latest cyber threats.
 - Secure your assets.
 - Let your IT Team focus on daily business operations.
- **People: Security Awareness & Training**
 - Example-based awareness program to focus on the risks and the role people play in cybersecurity. Perform quarterly.
 - IT Team training program on cybersecurity technology and incident response.
- **Process: Security Governance, Policies, and Planning**
 - Develop cyber risk management and data breach response plans.

+ Cyber Risk Management Plan

■ Why do I need this?

- Every company will be the victim of a breach at some point. Those that have taken steps to prepare for that day will be better able to detect, stop, and respond, and they will face less liability.

■ Where do I start?

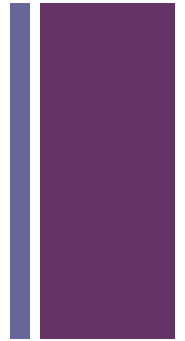
- Start at the top – discuss cybersecurity risk management with your BOD. Have your officers lead the implementation.
- Consider a cybersecurity insurance policy.

■ What's the next step?

- You need to determine your risks – they are different for every company.
- Consider your third party vendors.

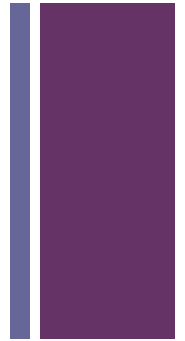
■ Do you regularly review existing policies?

- Many companies have never reviewed or updated existing record retention policies, CPNI policies, and security policies.





Cyber Risk Management Plan



- **But...some of this is expensive!**
 - If customers' private information is compromised, you will face an investigation and potentially an enforcement action. Government and Regulators are embracing a “risk management approach” to cybersecurity. If you can show you have taken steps to protect yourself, your exposure will be reduced.

- **I'm feeling overwhelmed.**
 - This is normal. Just get started. Put your plan in motion day-by-day and piece-by-piece.

- **When am I finished?**
 - You are never finished! It's an ongoing process! Your plan is a living document – it should evolve!

+ Cyber Risk Management Plan

Knowledge is Power

- **B&B Cybersecurity Compliance Planning Guide**
 - Cybersecurity Introduction, Risk Assessment, Security Solutions
- **CSRIC IV - Cybersecurity Risk Management and Best Practices Working Group 4: Final Report (March 2015)**
- **NIST Framework**
- **Critical Infrastructure Cyber Community C³ (pronounced “C Cubed”) Voluntary Program**
- **Where can I look for help?**
 - Talk to your peers.
 - Contact an expert.





Erin Fitzgerald

efitzgerald@bennetlaw.com

(202) 551-0060

QUESTIONS?

