Cybersecurity – Threats, Responses & Best Practices

BUTZEL LONG

Claudia Rast *Butzel Long* *rast@butzel.com*
Scott Bailey *N1 Discovery* *scott.bailey@n1discovery.com*
Stewart Nelson *Kapnick Insurance Group* *Stewart.Nelson@kapnick.com*

Managing Cyber Liability

FORENSICS,
LEGAL LIABILITIES,
INSURANCE, AND
BEST PRACTICES

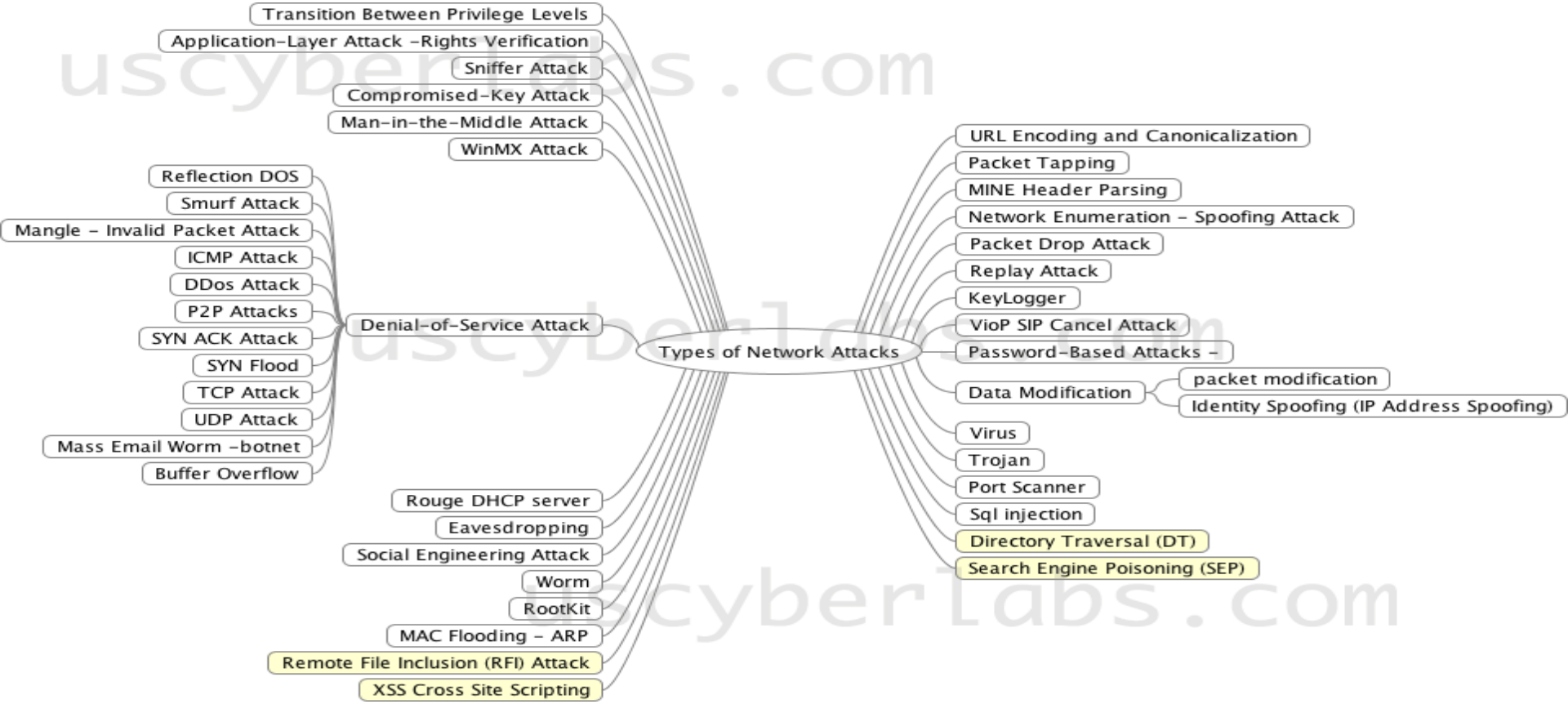
BUTZEL LONG

FORENSICS

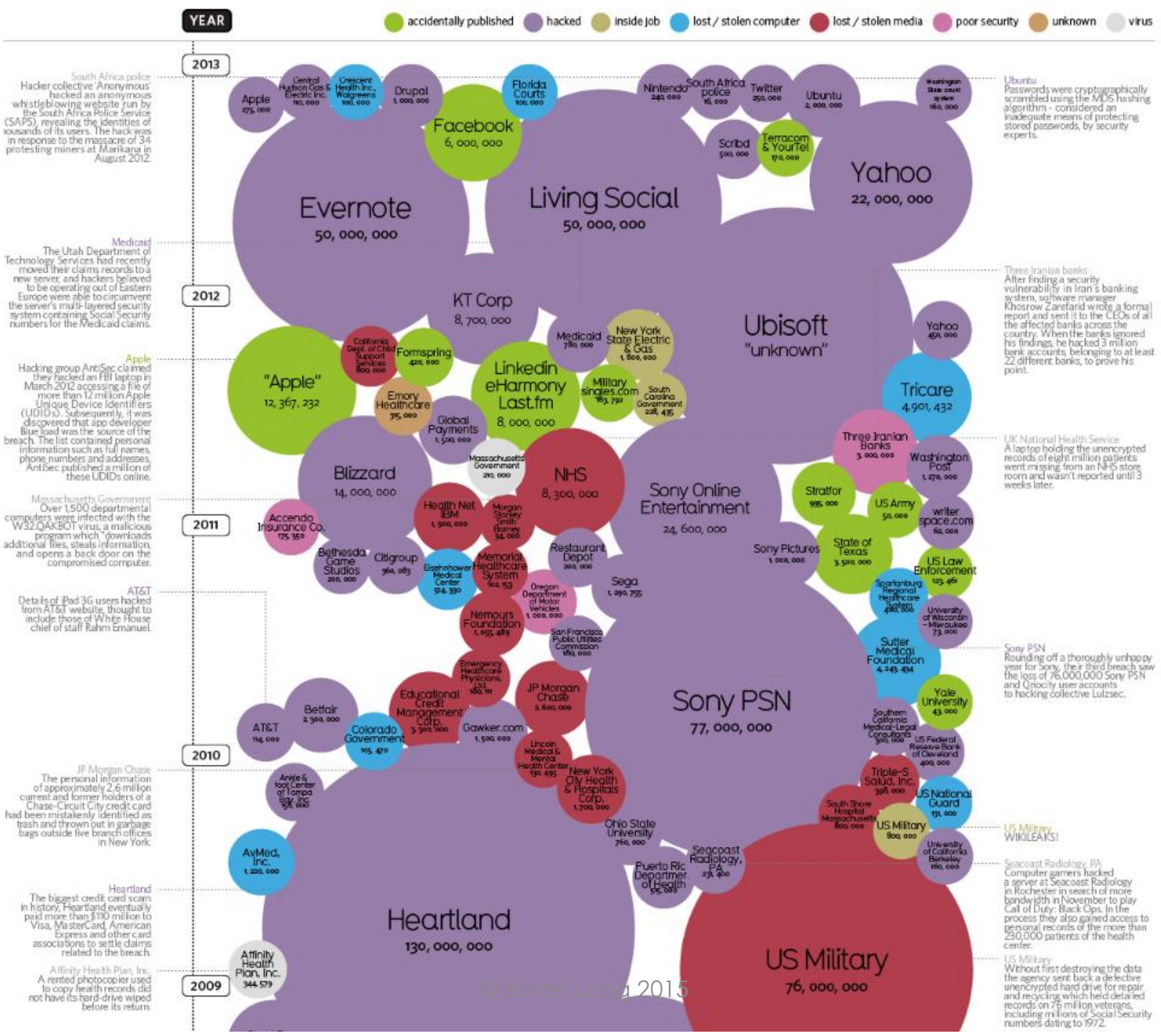
BUTZEL LONG

What Are the Threats?

From USCyberlabs.com



BUTZEL LONG


YEAR
accidentally published
hacked
inside job
lost / stolen computer
lost / stolen media
poor security
unknown
virus
2013
2012
2011
2010
2009
South Africa police
Hacker collective 'Anonymous' hacked an anonymous whistleblowing website run by the South Africa Police Service (SAPS), revealing the identities of thousands of its users. The hack was in response to the massacre of 34 protesting miners at Marikana in August 2012.
Medicaid
The Utah Department of Technology Services had recently moved their claims records to a new server, and hackers believed to be operating out of Eastern Europe were able to circumvent the server's multi-layered security system containing Social Security numbers for the Medicaid claims.
Apple
Hacking group AntiSec claimed they hacked an FBI laptop in March 2012 accessing a file of more than 12 million Apple Unique Device Identifiers (UDID's). Subsequently, it was discovered that app developer Blue Toad was the source of the breach. The list contained personal information such as full names, phone numbers and addresses. AntiSec published a million of these UDIDs online.
Massachusetts Government
Over 1,500 departmental computers were infected with the W32.QAKBOT virus, a malicious program which "downloads additional files, steals information, and opens a back door on the compromised computer.
AT&T
Details of iPad 3G users hacked from AT&T website, thought to include those of White House chief of staff Rahm Emanuel.
JP Morgan Chase
The personal information of approximately 2.6 million current and former holders of a Chase-Circuit City credit card had been mistakenly identified as trash and thrown out in garbage bags outside five branch offices in New York.
Heartland
The biggest credit card scam in history, Heartland eventually paid more than $110 million to Visa, MasterCard, American express and other card associations to settle claims related to the breach.
Affinity Health Plan, Inc.
A rented photocopier used to copy health records did not have its hard-drive wiped before its return.
Ubuntu
Passwords were cryptographically scrambled using the MD5 hashing algorithm - considered an inadequate means of protecting stored passwords, by security experts.
Three Iranian banks
After finding a security vulnerability in Iran's banking system, software manager Khosrow Zarefarid wrote a formal report and sent it to the CEOs of all the affected banks across the country. When the banks ignored his findings, he hacked 3 million bank accounts, belonging to at least 22 different banks, to prove his point.
UK National Health Service
A laptop holding the unencrypted records of eight million patients went missing from an NHS store room and wasn't reported until 3 weeks later.
Sony PSN
Rounding off a thoroughly unhappy year for Sony, their third breach saw the loss of 76,000,000 Sony PSN and Qriocity user accounts to hacking collective Lulzsec.
US Military
WIKILEAKS!
Seacoast Radiology, PA
Computer gamers hacked a server at Seacoast Radiology in Rochester in search of more bandwidth in November to play Call of Duty: Black Ops. In the process they also gained access to personal records of the more than 250,000 patients of the health center.
US Military
Without first destroying the data the agency sent back a defective unencrypted hard drive for repair and recycling which held detailed records on 76 million veterans, including millions of Social Security numbers dating to 1972.
Facebook 6,000,000
Evernote 50,000,000
Living Social 50,000,000
Yahoo 22,000,000
KT Corp 8,700,000
Ubisoft "unknown"
"Apple" 12,367,232
Linkedin eHarmony Last.fm 8,000,000
Blizzard 14,000,000
NHS 8,300,000
Sony Online Entertainment 24,600,000
Sony PSN 77,000,000
Heartland 130,000,000
US Military 76,000,000
Tricare 4,901,432
Apple 275,000
Central Hudson Gas & Electric Inc. 110,000
Crescent Health Inc., Walgreens 100,000
Drupal 1,000,000
Florida Courts 100,000
Nintendo 240,000
South Africa police 16,000
Twitter 250,000
Ubuntu 2,000,000
Washington State court system 160,000
Scribd 500,000
Terracom & YourTel 170,000
Yahoo 450,000
California Dept. of Child Support Services 800,000
Formspring 420,000
Medicaid 780,000
New York State Electric & Gas 1,800,000
Military singles.com 189,700
South Carolina Government 228,435
Emory Healthcare 315,000
Global Payments 1,500,000
Massachusetts Government 210,000
Three Iranian Banks 3,000,000
Washington Post 1,270,000
Stratfor 935,000
US Army 50,000
writer space.com 62,000
Accendo Insurance Co. 175,350
Health Net IBM 1,900,000
Morgan Stanley Smith Barney 34,000
Sony Pictures 1,000,000
State of Texas 3,500,000
US Law Enforcement 123,461
Bethesda Game Studios 200,000
Citigroup 360,083
Eisenhower Medical Center 514,330
Memorial Healthcare System 102,153
Restaurant Depot 200,000
Sega 1,290,755
Spartanburg Regional Healthcare System 400,000
University of Wisconsin - Milwaukee 73,000
Nemours Foundation 1,095,489
Oregon Department of Motor Vehicles 1,000,000
San Francisco Public Utilities Commission 180,000
Sutter Medical Foundation 4,243,434
Emergency Healthcare Physicians, Ltd 180,111
Educational Credit Management Corp. 3,300,000
JP Morgan Chase 2,000,000
Yale University 43,000
AT&T 114,000
Bet Fair 2,300,000
Colorado Government 105,470
Gawker.com 1,500,000
Southern California Medical-Legal Consultants 300,000
US Federal Reserve Bank of Cleveland 400,000
Lincoln Medical & Mental Health Center 130,495
New York City Health & Hospitals Corp. 1,700,000
Triple-S Salud, Inc. 398,000
US National Guard 131,000
Ohio State University 760,000
South Shore Hospital Massachusetts 800,000
US Military 800,000
University of California Berkeley 160,000
AvMed, Inc. 1,220,000
Puerto Rico Department of Health 595,000
Seacoast Radiology, PA 234,400
Affinity Health Plan, Inc. 344,579
© Butzel Long 2015

Who Are the Threat Agents?

- Corporations
- Cybercriminals (Mafia: Russia, Brazil, Mexico…)
- Insiders/Employees (Ed Snowden)
- Hacktivists (Anonymous, WikiLeaks)
- Nation-States (China, Russia, N. Korea)
- Terrorists (Al-Qaeda, ISIL)

CERT Insider Threat Profile

- >30% of Insider Saboteurs had prior arrest history (2011 study showed 30% of U.S. adults arrested by age 23)
- Behavior Issues: bragging about the damage they could do if they wanted (trigger: passed over for promotion)
- Using Company resources for side business or talking about competing business
- Coercing coworkers to get credentials
- Warning: >70% IP theft occurs w/in 30 days of announcing departure
- >50% Insider Saboteurs were former employee with access via "backdoors" or credentials that were never disabled

from Carnegie Mellon's Common Sense Guide to Mitigation Insider Threats, 4th Ed. Dec. 2012

More on Insider Threats

- Typically Three Main Categories
  - Sabotage (24%
  - Fraud (44%)
  - Theft of IP (16%)
- Most Often An Employee of Target Entity (85%)
- Most Activity Occurred During Work (72%) and at Work Site (70%)

from Carnegie Mellon's Insider Threat Blog, Oct. 17, 2013

What Do They Want?

- Money
- Information
- Mayhem

BUTZEL LONG

How Do They Get In?

- Poor Access Controls
- Improper/Weak Authentication
- Insufficiently Protected Credentials
- Poor Patch Management; Weak Testing
- No Defined Security Perimeter; Lack of Network Segmentation
- Improper Device Configuration; Poor Monitoring
- Lack of Security Audits, Logging Practices
- Weak Enforcement of Remote Login Policies

Once "In," What Can They Do?

- Create/modify/delete/execute programs
- Upload/download files
- Create/delete/directories
- List/start/stop processes
- Modify system registry
- Take screenshots of user's desktop
- Capture keystrokes
- Capture mouse movements
- Start interactive command shell
- Create a remote desktop interface
- Harvest passwords
- Enumerate users
- Enumerate other systems on the network
- Set system to "sleep" (go inactive)
- Log off the current user
- Shut down the system

Trends / Predictions

- Hacking as a service.
- Ransomware (data encryption-extortion).
- Smartphone kidnapping.
- Increase in social engineering attacks.
- Increase in music and movies to install malware.
- Hackers will continue to use and abuse cloud services.
- Mobile threats and more mobile threats.

LEGAL LIABILITIES

BUTZEL LONG

Legal Liabilities

- Defining the Breach/Security Incident
- When the Breach/Security Incident Happens
- Liability for Breach/Security Incident : What Laws?
- Recent Headlines
- The Costs of Breach
- Current Legislative Activities

Defining the "Breach"

- First: What is a Breach/Security Incident?
  - A violation or "imminent threat of violation" of computer security policies, acceptable use policies, or standard security practices
    - An "imminent threat of violation" → a situation when entity has a factual basis for believing that a specific incident is about to occur, e.g., notice from a software vendor warning of new malware that is rapidly spreading across the Internet
  - An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash
  - Users are tricked into opening a "quarterly report" sent via email that is actually malware; running the tool infects entity's computers and established connections with an external host
  - An attacker obtains sensitive data and threatens to publish details if the organization does not pay a designated sum of money
  - See Federal Incident Reporting Guidelines at: http://www.us-cert.gov/government-users/reporting-requirements
- Second: What was Disclosed, Published, Stolen, Accessed without Authority, Not Properly Secured…

Liability for Breach—What Laws?

- Criminal Code—Title 18
  - Computer Fraud & Abuse Act, 18 U.S.C. § 1030
  - Wiretap Act, 18 U.S.C. § 2511
  - Stored Communications Act (unlawful access), 18 U.S.C. § 2701
  - Identity Theft, 18 U.S.C. § 1028(a)(7) & § 1028A
  - Electronic Communications Privacy Act, 18 U.S.C. § § 2510-2522
  - Economic Espionage Act, 18 U.S.C. § § 1831-1839
- Administrative Statutes—Title 16
  - Electric Reliability Provision of Federal Power Act 16 U.S.C. § 824o(b) (2006)
    - Gave FERC authority to enforce compliance with reliability standards for bulk power system, including protection from cybersecurity incidents
- Other Federal Law & Regulations: HIPAA/HITECH (Healthcare), FTC Act (Online Commerce), GLB & OCC (Financial)
- State Data Breach Laws; Payment Card Industry – PCI Industry-Enforced
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity Feb 2014 (Cybersecurity Framework (NIST Standard) Feb 2014)

Recent Headlines: Sony & Morgan Stanley

- Sony
  - FBI confirms (with saying too much) that N. Korea was behind the Sony Hack
  - Turns out the US has been inside N. Korea's network since 2010
  - Sony was target of Spearphishing attack beginning in September 2014 that was implemented system-wide in November 2014
- Morgan Stanley
  - Unwitting and too curious financial advisor finds way to access 350,000 records (out of 3.5 Million total records) from wealth management system
  - On Dec. 27th, records of 900 wealthiest clients were posted on online bulletin board Pastebin
    - Promised more information in exchange for 78,000 "speedcoins" (worth about $2.95)
  - Morgan Stanley's data loss prevention system caught employee's breach within 8 hours

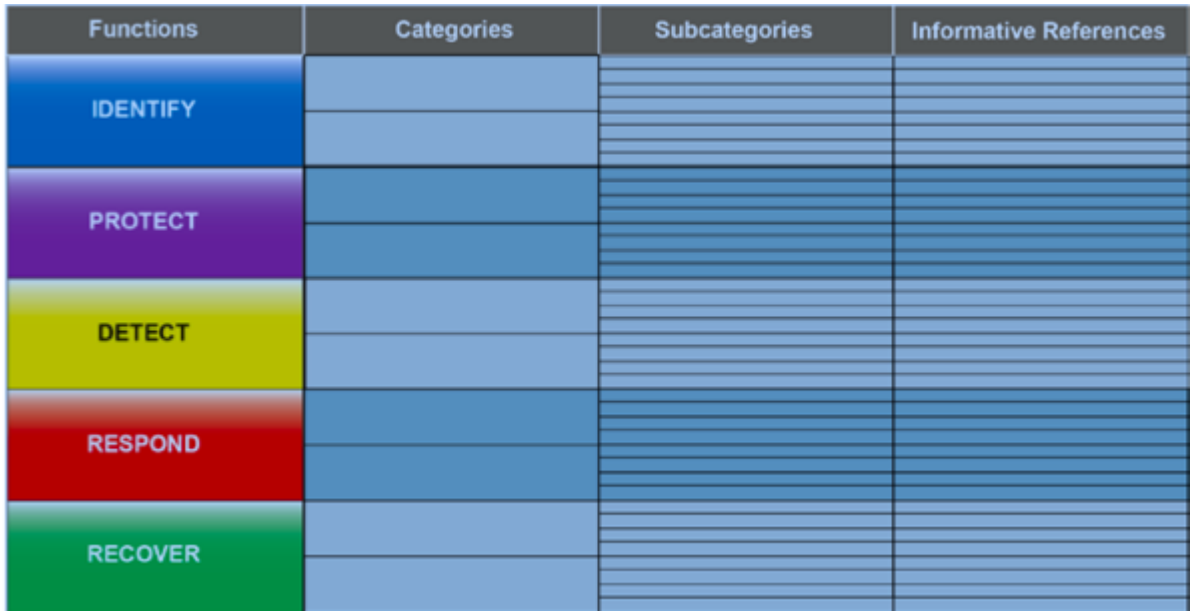
Breach Costs & Risk Protection

- Average cost per compromised record in 2014: $201
  - For “malicious” attacks: $246/record
  - Compare: Average cost per compromised record in 2010: $210
  - Average cost per compromised record in 2006: $138
- Companies with Incident Response Plan in place
  - Paid $17 less per compromised record
- Companies who alerted customers too soon
  - Paid $15 more per compromised record
- Building the Effective Cyber Risk Culture (DHS May 2013)
  - engaged executive leadership
  - targeted cyber risk management and awareness
  - cost-effective technology investments tailored to organizational needs
  - relevant cyber risk information sharing

Current Federal Activities

- FTC is increasingly more aggressive in targeting companies who profess security, but don't deliver: e.g., SnapChat, Wyndham (misrepresenting security measures)
- House version of Cybersecurity Information Sharing Act of 2014 reintroduced January 2015
- President Obama drafted similar proposed legislation and signed Executive Order Feb 13, 2015, promoting private sector information sharing
- Hurdles for any legislation:
  - Defining adequate consumer protection
  - Information sharing
  - liability protection
  - Antitrust protection

Cybersecurity Framework: Core Functions



BUTZEL LONG

Sources, Targets & Risks: It's Us!

Source

- Mobile Computing *(controlling BYOD)*
- Social Media *(online & customer service)*
- Big Data

Target

- Critical Infrastructures *(electric, oil, gas, water, traffic, ports, chemical)*
- Trust Infrastructures *(finance, insurance, accounting, legal)*
- The Cloud *(who owns, who controls, where located)*

Risks

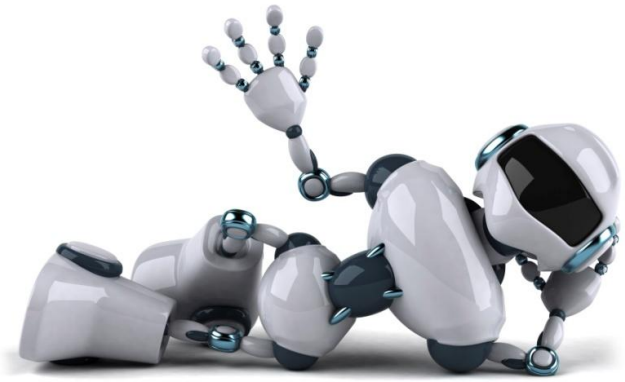
- Communication Breach: Data Center → ≠ Board Room
- Target Breach: Auto Breach Detection turned "Off" by IT

INSURANCE

BUTZEL LONG

7 Components of Cyber Liability Policies

1. Data Breach: Failure to protect an individual's privacy – 1st Party Costs , Notification, Forensics, Legal Assistance, Credit Monitoring, PR Firms.
2. Data Breach: Failure to protect an individual's privacy – 3rd Party Costs, Defense Costs & Settlements
3. Network Security: Loss or damage to a network & data, 1st & 3rd Party (may include lost income)
4. Media Liability: Web content (Libel, Defamation)
5. Fines & Penalties (HIPAA, PCI)
6. eVandalism & Extortion
7. Property loss from Cyber Perils (Internet of Things)



BUTZEL LONG

1. Data Breach: 1st Party (Insured's) Expenses May Cover

- ✓Legal services
- ✓Forensic reviews
- ✓Notification to third parties
- ✓Credit monitoring
- ✓Credit freezes
- ✓Call centers
- ✓Public relations

- Reimbursement or Captive services
- Trigger is Potential Loss of Information
- Sometimes sub-limited

2. Data Breach: 3rd Party Protection

- Civil Suits: 3rd Party Claims for Privacy Claims
  - Court & defense costs, settlements, appeals, expert witnesses etc.
  - May include 3rd Party Business Income.)
- Arbitration, Administrative Hearings & Investigations
- Violation of Federal (Domestic or Foreign) or State regulations
- Trigger is Wrongful Act or Personal Injury

3. Network Security: Data & Hardware Restoration

- Loss of or damage to insured's or other's network or data
- Reasonable & necessary expenses that are required to restore the network and/or data
- May include 1st and 3rd Party Business Income

BUTZEL LONG

4. Media Liability (Web Content)

- Copyright, slogan, trademark, trade or service name
- Emotional distress
- Libel, slander/defamation, product disparagement
- Invasion of privacy
- Plagiarism, failure to attribute
- Misstatement or misleading statement
- Failure to follow published privacy policy
- Wrongful entry or eviction
- Contextual errors and Omissions

BUTZEL LONG

5. Fines & Penalties: Sometimes called “Regulatory”

- HIPPA-HITECH
- Payment Card Industry, PCI (Credit cards)

Usually sub-limited

BUTZEL LONG

6. eVandalism & Cyber Extortion

- Loss - Money paid to terminate threat
  - ❖ Cost to investigate
  - ❖ Travel expenses
- Trigger is the threat→ Loss

BUTZEL LONG

7. Property Damage from Cyber Perils

- New Coverage Forms just Released
- Can include Bodily Injury "Kinetic" Injury
- Covers Internet of Things
  - Virus damages your refrigerator
  - Malware in your heart-lung machine
  - Hackers attack your driverless car

BUTZEL LONG

BEST PRACTICES

Best Practices for Management

- Perform Risk Assessment (Physical Plant, Information Systems & Workforce)
- Segregate & Secure High Risk Information, Operations & Workers
- Encrypt Sensitive Data/Implement Robust Password Policy
- Implement Company-wide Training (Ongoing)
- Incorporate Security By Design (i.e., from the beginning)
- Acquire Cyber Liability Insurance
- Enable Network Security Monitoring & Review of Log Files (Lesson Learned from Target)
- Demand Compliance from Contractors & Suppliers (Another Lesson from Target)
- Conduct Table-Top Drills
- Have Experts at the Ready If/When an Attack Occurs

Best Practices for Companies

- Restrict Remote Access
- Enforce Password Policies
- Restrict Activities on POS Systems to Sales
- Deploy Anti-Virus Systems on POS
- For Large, Multi-Store Companies
  - Segment POS Network from Corporate Network
  - Monitor Network Traffic from POS to Network
  - Use Two-Factor Authentication

Best Practices for IT Departments

- Eliminate Unnecessary Data
- Conduct Ongoing & Active Risk Analysis
- Collect, Analyze & Share Incident Data
- Collect, Analyze & Share Tactical Threat Intelligence, Especially Indicators of Compromise
- Focus on Better & Faster Detection
- Establish Metrics: “Number of Compromised Systems” & “Mean Time To Detection” in Networks; Use Metrics to Drive Security
- Evaluate Threat Landscape to Prioritize Treatment Strategy (It’s not a “One-Size Fits All” World)
- Track Workforce: Who’s Who, What they Do & When they Go

Questions

Claudia Rast	Scott Bailey	Stew Nelson
Butzel Long	N1 Discovery	Kapnick Insurance Group
rast@butzel.com	scott.bailey@n1discovery.com	Stewart.Nelson@kapnick.com

BUTZEL LONG