Cybersecurity – Threats, Liabilities & Best Practices

April 21, 2016

Claudia Rast

Butzel Long

Ann Arbor, MI

rast@butzel.com

Managing Cyber Liability

PRIVACY vs SECURITY,
FORENSICS,
LIABILITIES,
INSURANCE, AND
BEST PRACTICES

"Data Privacy" and "Data Security"

- ***Data Privacy***: the relationship between the collection, storage, use, dissemination and security of information identifiable or defined as private, the varying public expectations (or not) of privacy, and the attendant legal and political tensions
- ***Data Security***: the protection of data from any unauthorized access in violation of policy, law, regulation or rule

Data Privacy: The States

- 50 States… 47 Different laws
- State “Right to be Forgotten” bills
- April 17, 2015: Delaware Attorney General proposes adoption of crime victim confidentiality and California style Student Data Privacy and Protection act

Data Privacy: Federal

- US is one of only two developed nations without privacy protections for all personal data (Turkey is the other one)
- Consumer Bill of Rights Act of 2015
  - Based on Fair Information Practices Principles (going back to 1974)
  - Would require companies to use "concise and easily understandable language" in privacy policies
- Data Security and Breach Notification Act of 2015
  - No private right of action
  - Seen by advocates as a "dumbing down" of state law

Data Privacy: EU and Global

- The Safe Harbor Agreement (and its end)
  - Now the “Privacy Shield”; June 2016 targeted for adoption
- EU “Right to be Forgotten”
- EU Data Privacy legislation to require explicit consent based on Snowden
- Germany proposes data privacy law allowing consumers to bring class actions for breaches and violation of privacy

The State of Cybersecurity

- Security flaws abound → zero day vulnerability
  - –Previously unknown security flaw
- CFO's are increasing spending on security
  - – 90% increased spending on new tools
  - – 72% created a formal response plan
  - – Almost 50% have turned to outside experts
- Law Firms are woefully behind (1.9% spend on security)
- Professional Service Firms serve as Bad Guy Gateways

Current Federal Activities

- Cybersecurity Information Sharing Act of 2015
  - President Obama signed December 18, 2015
- Requires DNI, DHS, DOD, and DOJ to develop and promulgate procedures to promote:
  - the timely sharing of classified and declassified cyber threat indicators in possession of the federal gov't with private entities, non-federal gov't agencies, or state, tribal, or local governments;
  - the sharing of unclassified indicators with the public;
  - the sharing of cybersecurity threats with entities to prevent or mitigate adverse effects
- Permits private entities to detect, prevent, or mitigate
  - Broadens private company activity formerly restrained by Electronic Communications Privacy Act of 1986
- Certain antitrust exemption for "cybersecurity purposes"
- DOJ to review privacy and civil liberties guidelines
- Provides liability protection if acting "in accordance with Act"

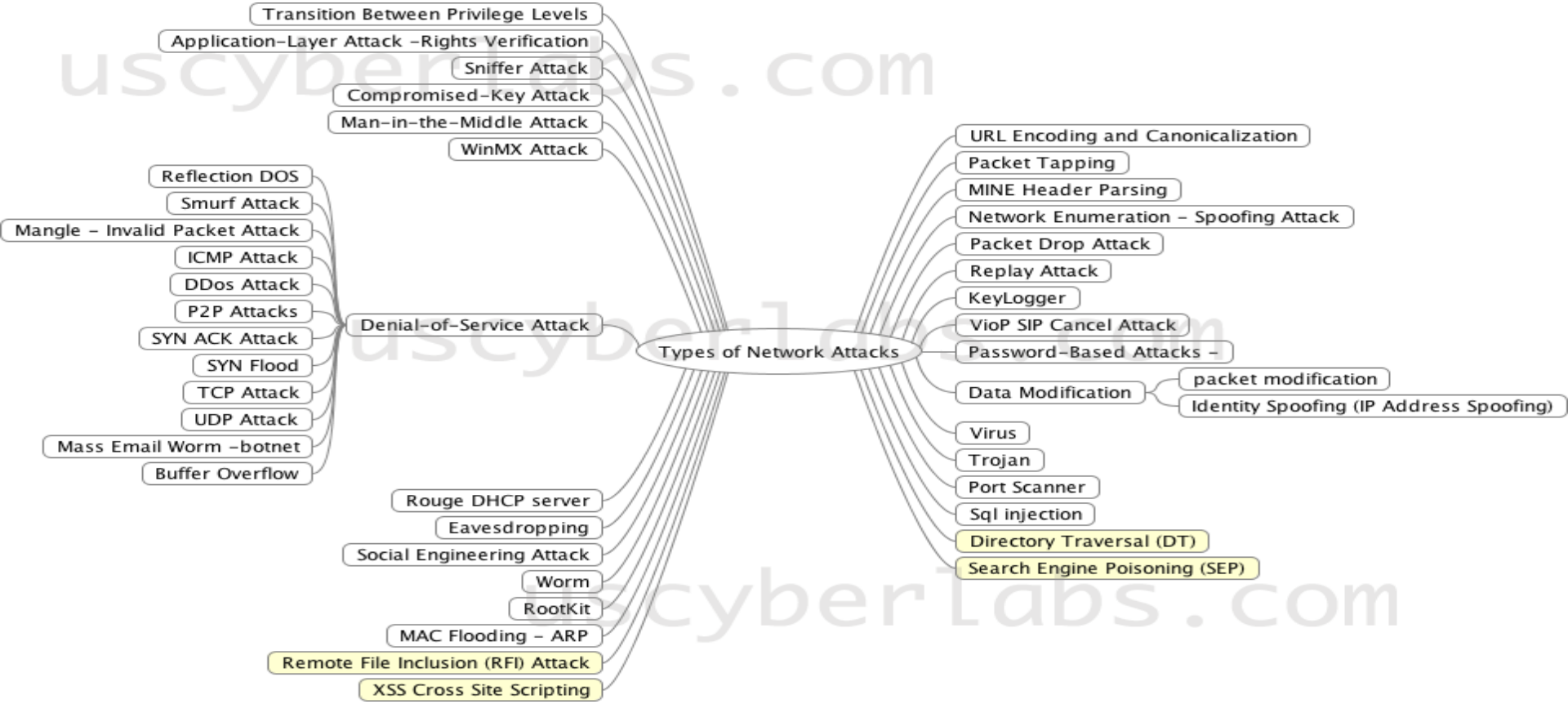
Current International Activities

- EU Court of Justice Struck Down Safe Harbor Framework on October 6, 2015
- The Court ruled as "invalid" the European Commission's Decision 2000/520/EC of 26 July 2000 "on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce."
- US Companies with EU locations & employees in flux:
  - *"In the current rapidly changing environment, the Department of Commerce will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework.* ***If you have questions, please contact the European Commission, the appropriate European national data protection authority, or legal counsel." export.gov website***
- **Keeping PI in EU across all economic sectors? →1% GDP**

FORENSICS

What Are the Threats?

From USCyberlabs.com



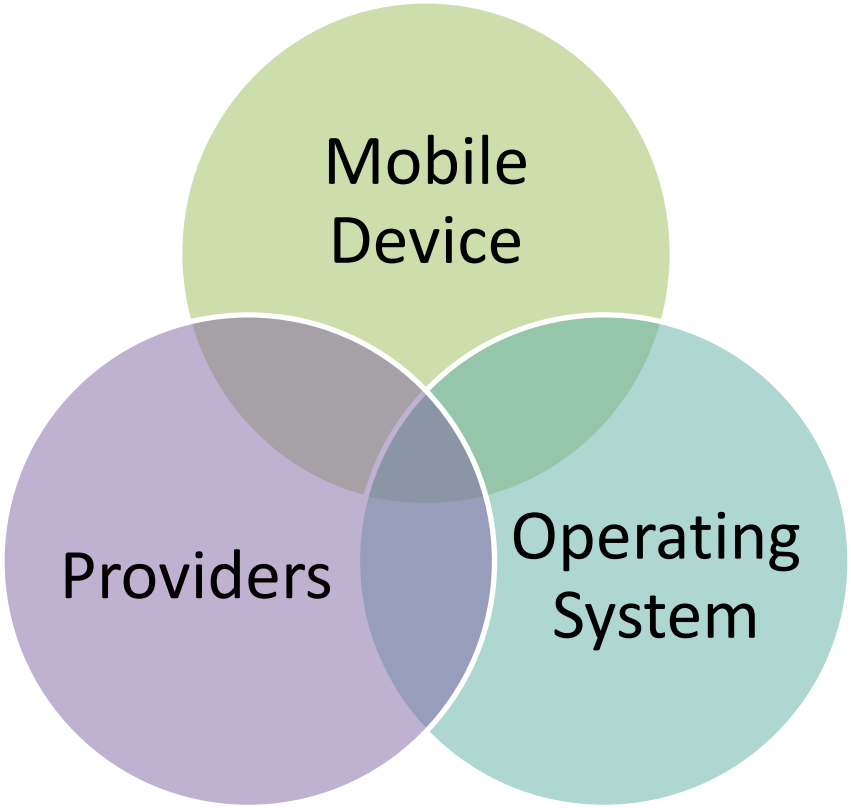
Who Are the Threat Agents?

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

What Do They Want?

- Money
- Information
- Mayhem

The Many Ways to Get "In"



- Device Theft/Loss
- Misuse of Camera/Mic/ GPS
- Device Configuration
- Poor Passwords
- Preboot Malware Alters OS
- Faulty OS (Zero-Day vulnerability)
- Malware Injection
- ID Theft (esp. w/same Password across apps)
- Policy Failure (Company; ISP, etc.)

Once "In", What Can They Do?

- Create/modify/delete/exe-cute 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

Terms to Review

- Security/Privacy Representations
- What type of Data
- Compliance with Laws (US, EU?)
  - Privacy Shield/Data Privacy
- Indemnification
- Insurance (Cyber Liability Coverage)
- Server Locations
  - In state? Out of state? Out of the country?
- Security protocols for breach notification

App Vulnerabilities

Buy at the Company Store!

- iTunes
- Android Market
- Microsoft

- Strict controls are in place for Apps sold in these venues

Be Wary in the Android World

- PC Mag Report 10/6/13: Trend Micro Labs reveal Android Malware reaches One Million
- One Billion Android phones vulnerable to “Stagefright”
  - Oct 2015

Cybersecurity Trends

- Hacking as a service
- Ransomware (data encryption-extortion)
- Smartphone kidnapping
- Increase in social engineering attacks
- Increase in music and movies to install malware
- Hackers abusing cloud services
- Increase in mobile threats

Case Study Examples

Professional Service Firm

- Admin Accesses Online Bank Acct
- "Delay" in connection
- Email Confirmation from Bank
- Local Police / Local IT
- Forensic "Mess" caused by too many "footprints and cleanups" by Police and IT
- Reporting Obligations?

Medical Device Provider

- Email from Ransomware
- Encryption of Company Data
  - Backup only 5 hours old
- 3rd Party Consultant tries to "Fix"
- Local IT calls FBI
- Unexplained Exfiltration
  - Mislabeled Servers
  - One-way log files
  - No Firewall
- Reporting Obligation?

LIABILITIES

Sources, Targets & Risks: It's Us!

Source

- Mobile Computing *(controlling BYOD)*
- Social Media *(online & customer service)*
- 27% Employees would sell passwords
  - 2016 SailPoint Market Pulse Survey

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

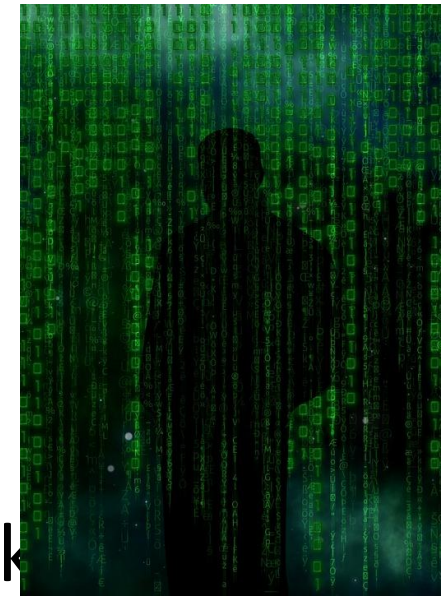
CERT Insider Threat Profile

- More than 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
- ***More than 70% IP theft occurs within 30 days of employees announcing departure***
- More than 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

Liabilities

- Defining the Breach/Security Incident
- Liability for Breach/Security Incident : What Laws?
- Corporate Board
- Cyber Risks for Law Firms

What is a Breach?

- First: What is a Breach?
- Second: What was Disclosed, Published, Stolen, Accessed without Authority, Not Properly Secured…
- Federal Law & Regs: HIPAA/HITECH (Healthcare), FTC Act (Online Commerce), GLB & OCC (Financial)
- State Data Breach Laws (47 plus D.C., Puerto Rico, Virgin Islands & Guam)
- Other: Payment Card Industry
- Cybersecurity Framework (NIST Standard)
  - Connecticut, Maryland, Hawaii

Detection: Searching for Anomalies and Events

- Understand a baseline of your network operations – what is “normal” for users and systems?
- Assess unusual or anomalous events including system use and malicious code
- Determine the impact of the event
- Elevate events to key personnel
- CISA and Monitoring/Sharing

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 (47 states plus DC, Puerto Rico, Virgin Islands)
- Payment Card Industry – PCI Industry-Enforced

Corporate Board Liability

There is increasing importance for corporate boards (CISO) to take responsibility for cybersecurity issues.

SEC Commissioner Luis Aguilar: boards are a critical part of risk management in cybersecurity.

FINRA and FTC have an interest in boards working to mitigate security risks.

NIST finds board involvement critical to successful implementation of the framework.

The Risks to Law Firms & Service Providers

- In 2012, Mandiant estimated that 80% of the 100 largest US law firms were subject to successful data breaches by malicious intruders in 2011.
- March 4, 2016: FBI sends Private Industry Notification
  - "Criminal-Seeking-Hacker" Requests Network Breach for Inside Trading Operation
  - Financially motivated insider trading scheme targets international law firm information
  - Monitoring for material non-public information
- Panama Papers—40 years of client data

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
  - Engage executive leadership
  - Target cyber risk management and awareness
  - Implement cost-effective technology investments tailored to needs
  - Adopt relevant cyber risk information sharing

The Costs of Breach: Target Example

- Data Breach in Nov-Dec 2013
- 40 Million Credit Card Holders
- 110 Million Total PII Compromised
- CIO fired; CEO fired; $148M in losses (2014)
- March 2015 Settlement: $10M Escrow for Victims
  - must meet criteria & apply
  - $10,000 max per victim
- April 2015 Settlement: $19M to MasterCard
  - Maintain Written Security Program
  - Appoint CISO
  - Train Employees on Security Program

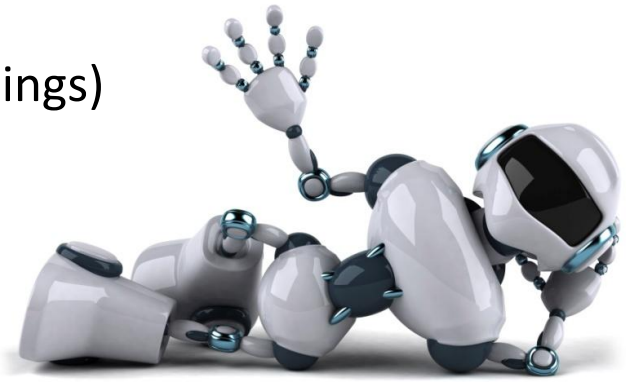
Risk Assessment Checklist

- ✓ Encryption
- ✓ Robust Firewalls
- ✓ Geolocation Filters—Geoblock Countries
- ✓ Backups
- ✓ Current Network Diagrams
- ✓ Accurate Server Labels
- ✓ Log Files
- ✓ Monitoring Exfiltration
- ✓ Employee Certifications

INSURANCE

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)

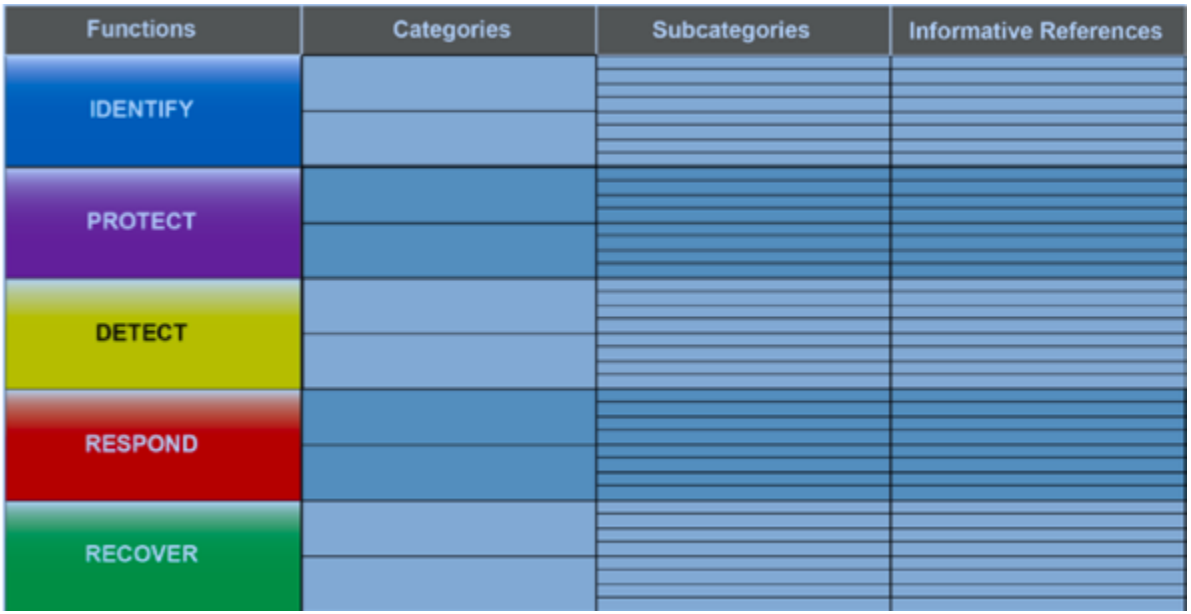


BEST PRACTICES

Current Federal Standard: NIST

NIST Cybersecurity Framework:

- Identify
- Protect
- Detect
- Respond
- Recover



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

Cybersecurity – Threats, Liabilities & Best Practices

Thanks! Questions?

April 21, 2016

Claudia Rast
Butzel Long
Ann Arbor, MI
rast@butzel.com