How to Improve Data Security and Reduce Potential Liability for Data Breaches

Randy Gainer, Attorney, CISSP

February 12, 2014

Davis Wright Tremaine LLP

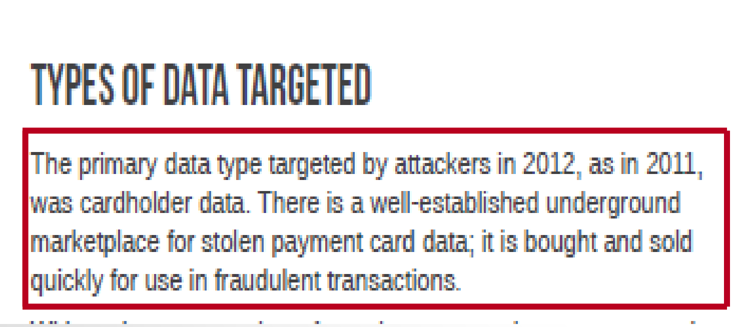
DEFINING SUCCESS TOGETHER

Topics

- The risks of cyber attacks
  - Identifying threats
  - Conducting risk assessments
- Choosing cost-effective security measures
- Evaluating cyber insurance coverage

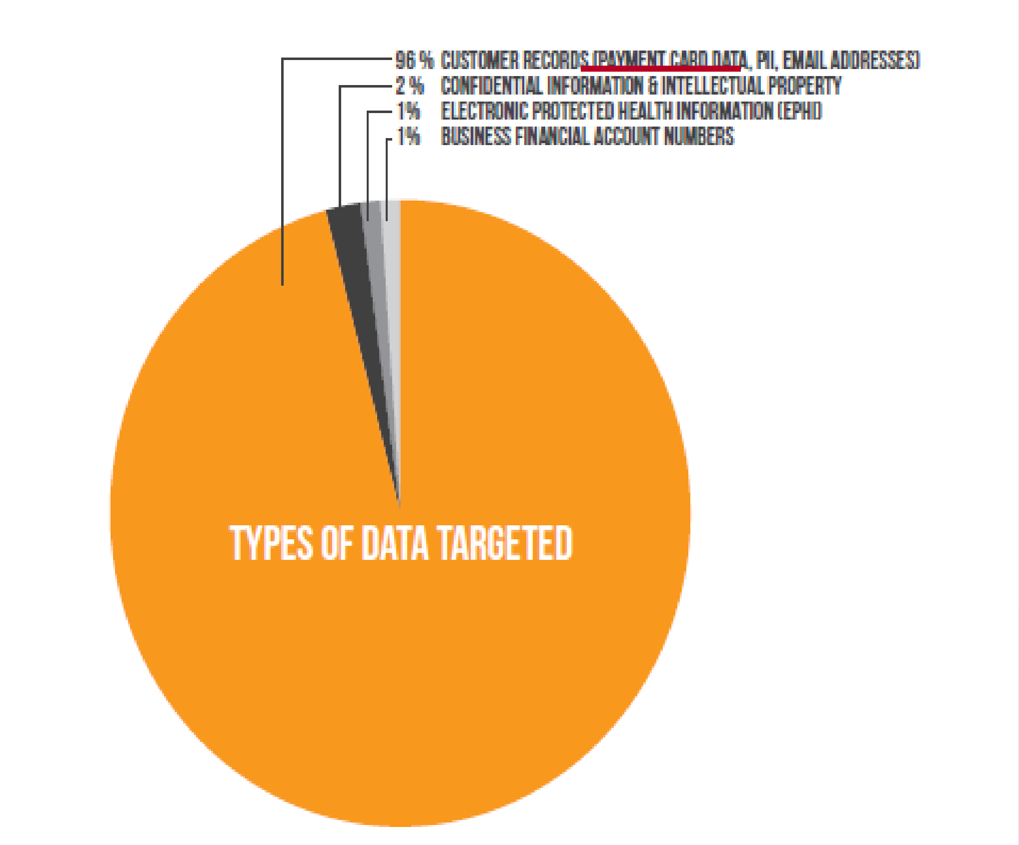
Identifying threats

- If your business processes payment cards, card data thieves are targeting your customers' card data:



TYPES OF DATA TARGETED

The primary data type targeted by attackers in 2012, as in 2011, was cardholder data. There is a well-established underground marketplace for stolen payment card data; it is bought and sold quickly for use in fraudulent transactions.



Trustwave 2013 Global Security Repor

Identifying threats

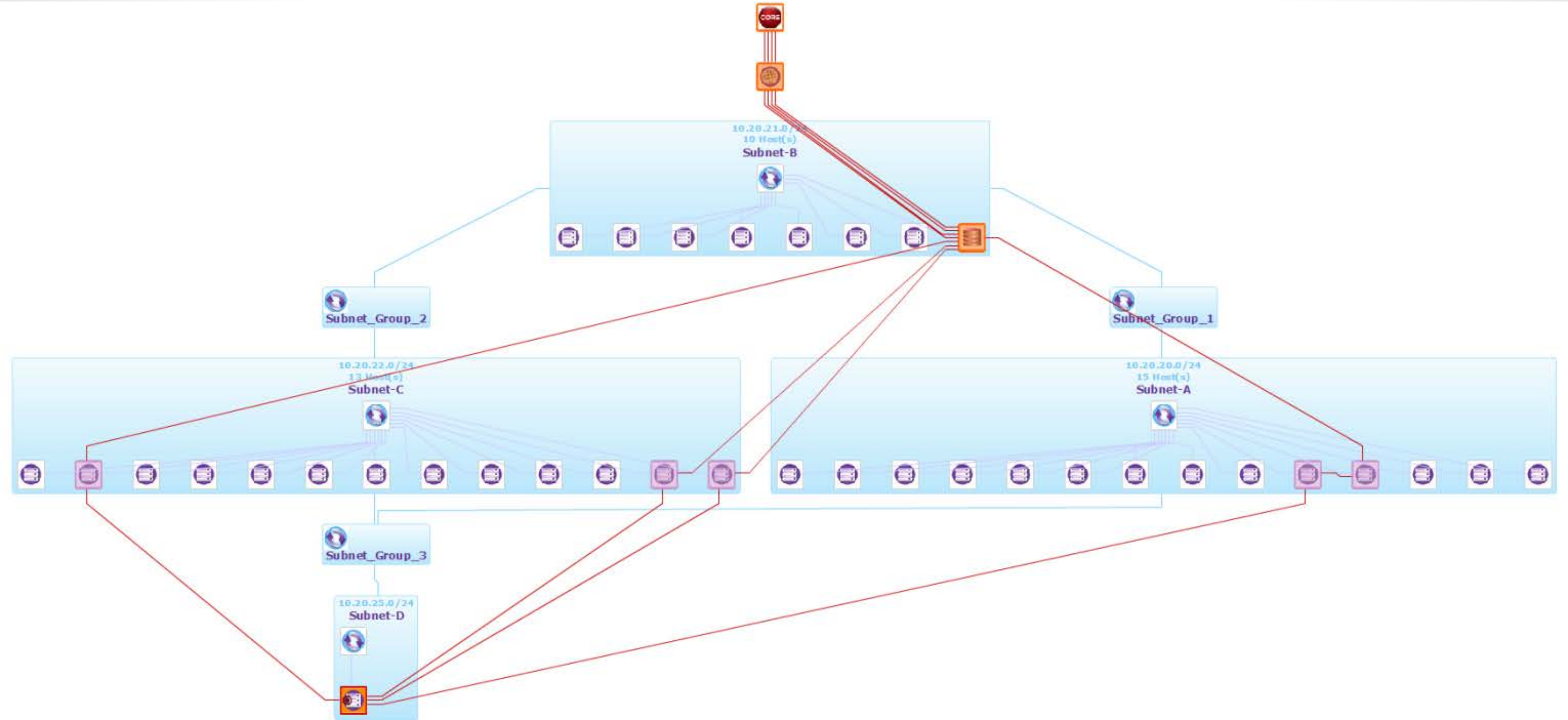
- **Targeted malware**
  - Deployed by phishing, poisoned websites, poisoned ads, watering hole attacks, and poorly protected third-party access tools. E.g.,
    - Remote access accounts for service vendors that rely on weak passwords; and
    - Phished credentials for access to the cardholder data environment (“CDE”).

Identifying threats

- **Targeted malware**
  - Programmed to **find, copy, store, encrypt, and exfiltrate payment card data**
  - Customized to avoid detection
  - Allows attacker to persistently communicate with, and exercise command and control of, the malware inside the target network
  - Permits an attacker to adapt to defenses (e.g., installs multiple backdoors to maintain attacker's access).

Identifying threats

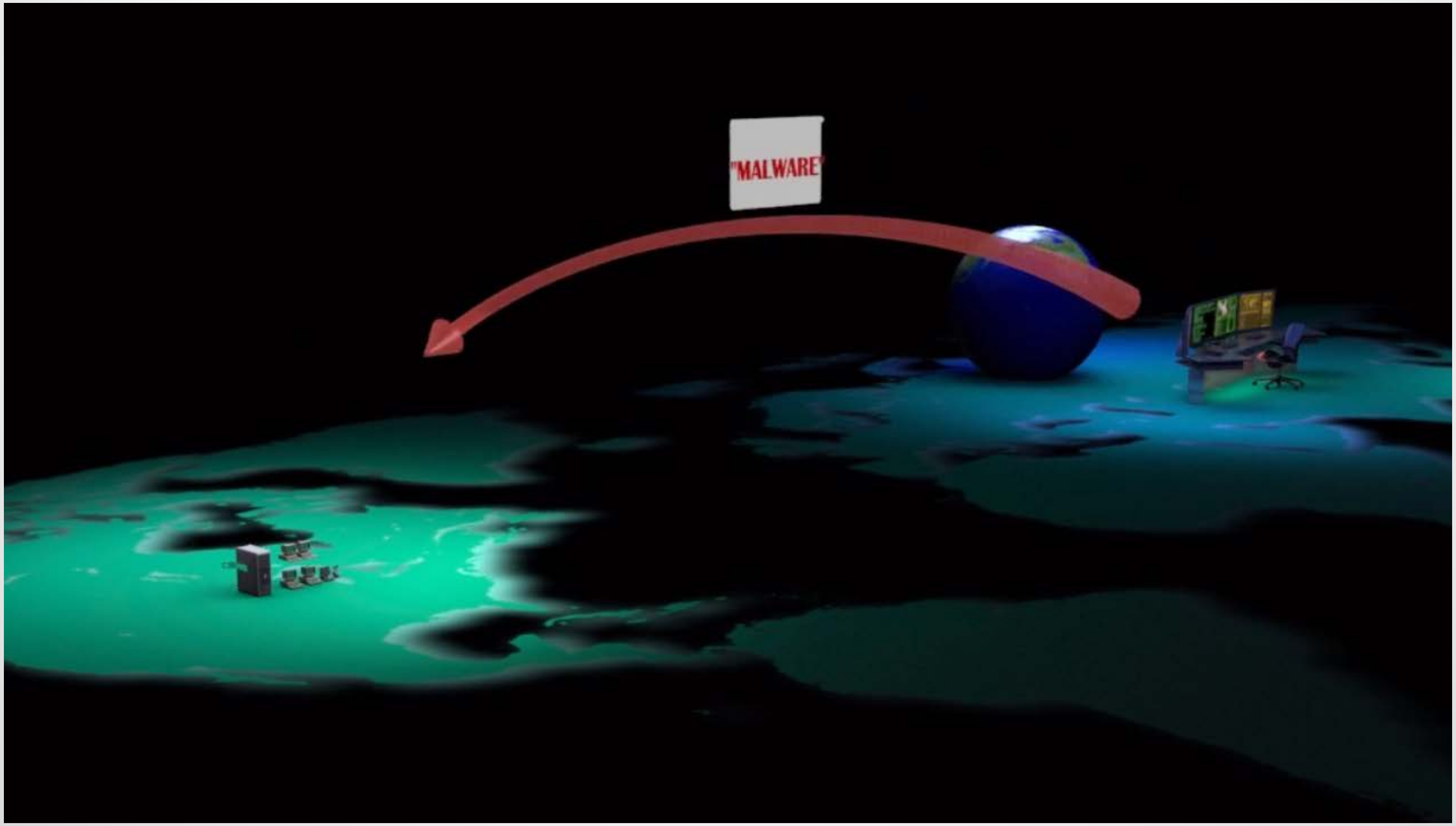
- **Targeted malware**
  – Used to find assets on the network to steal:



CORE SECURITY Thinking ahead Insight Enterprise Intelligence tool. Used with permission.

Identifying threats

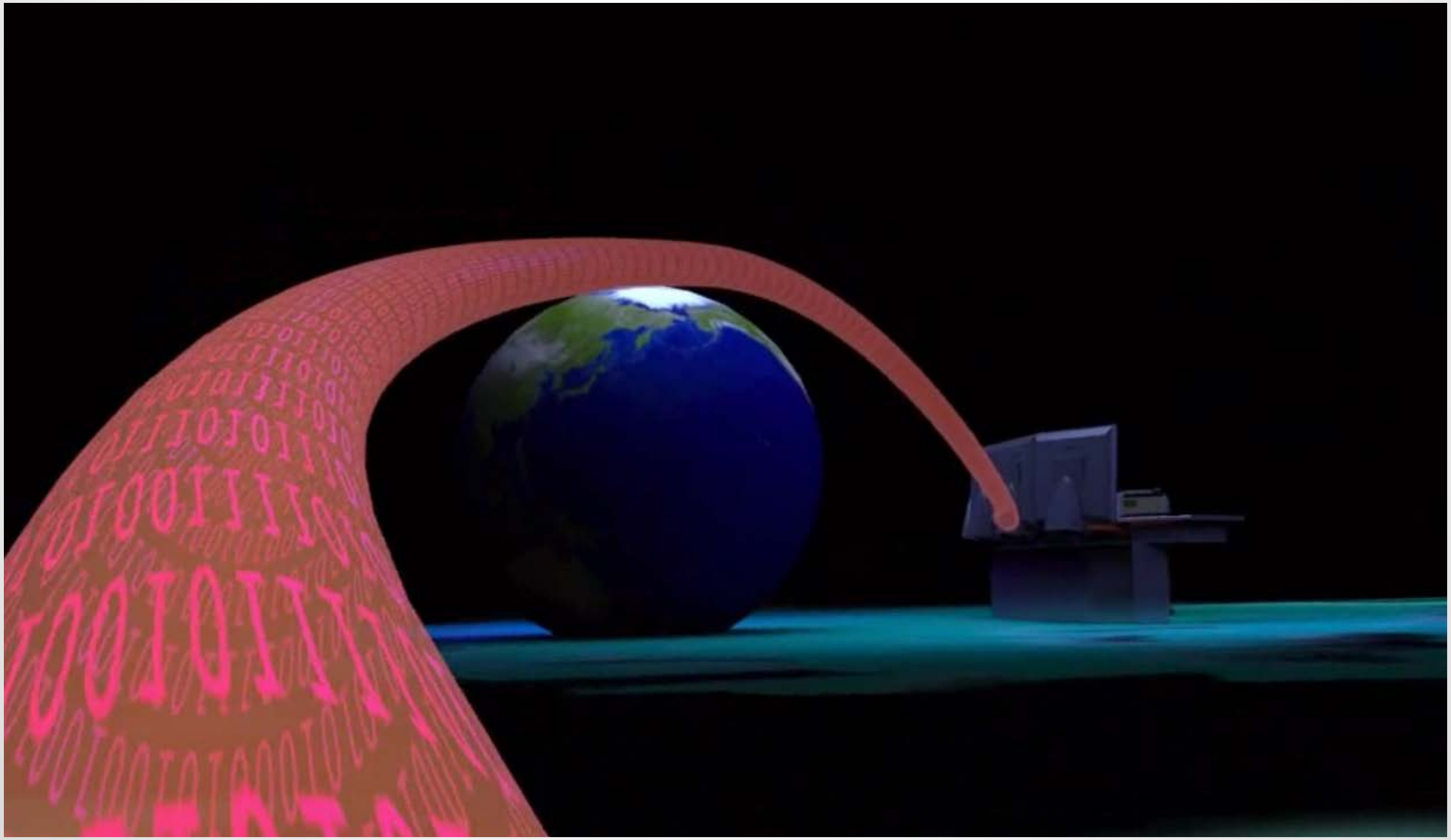
Identifying threats



Identifying threats

Identifying threats

Identifying threats



Identifying threats

Identifying threats

- Issuers, merchants, and acquirers of credit, debit, and prepaid cards experienced gross fraud losses of **$11.27 billion** in 2012, **up 14.6%** over the prior year.
- **Card issuers lost 63%** and merchants and acquirers lost the other 37%.

Business Wire, August 19, 2013, citing *The Nilson Report.*

Identifying threats

- Global Payments, Inc. (payment processor, 2012)
  - **1.5 million card data sets stolen**
  - **$121.2 million total losses** through mid-2013 (10/1/13 10-Q) (offset by $20 million in insurance payments) including
    - **$105.5 million** in professional **fees**, investigation and **remediation costs**, incentive payments to business partners, and credit monitoring and identity-protection insurance costs.
    - **$35.7 million** card brand **fines and assessments**.

Identifying threats

- TJX Companies, Inc.; 2007 retailer breach
  - **45.7 million card data sets stolen**
  - **$256 million total losses** (8/15/2007 *Boston Globe* article), including
    - Settlements of 27 lawsuits brought by more than 200 issuing banks:
      - **$40.9 million - Visa** and banks (*USA Today* report);
      - **$24 million - MasterCard** and banks (TJX press release)
      - **$9.75 million - State attorneys general** (*Computer World*)
  - Unspecified – customer class-action claims (TJX 9/21/07 8-K)

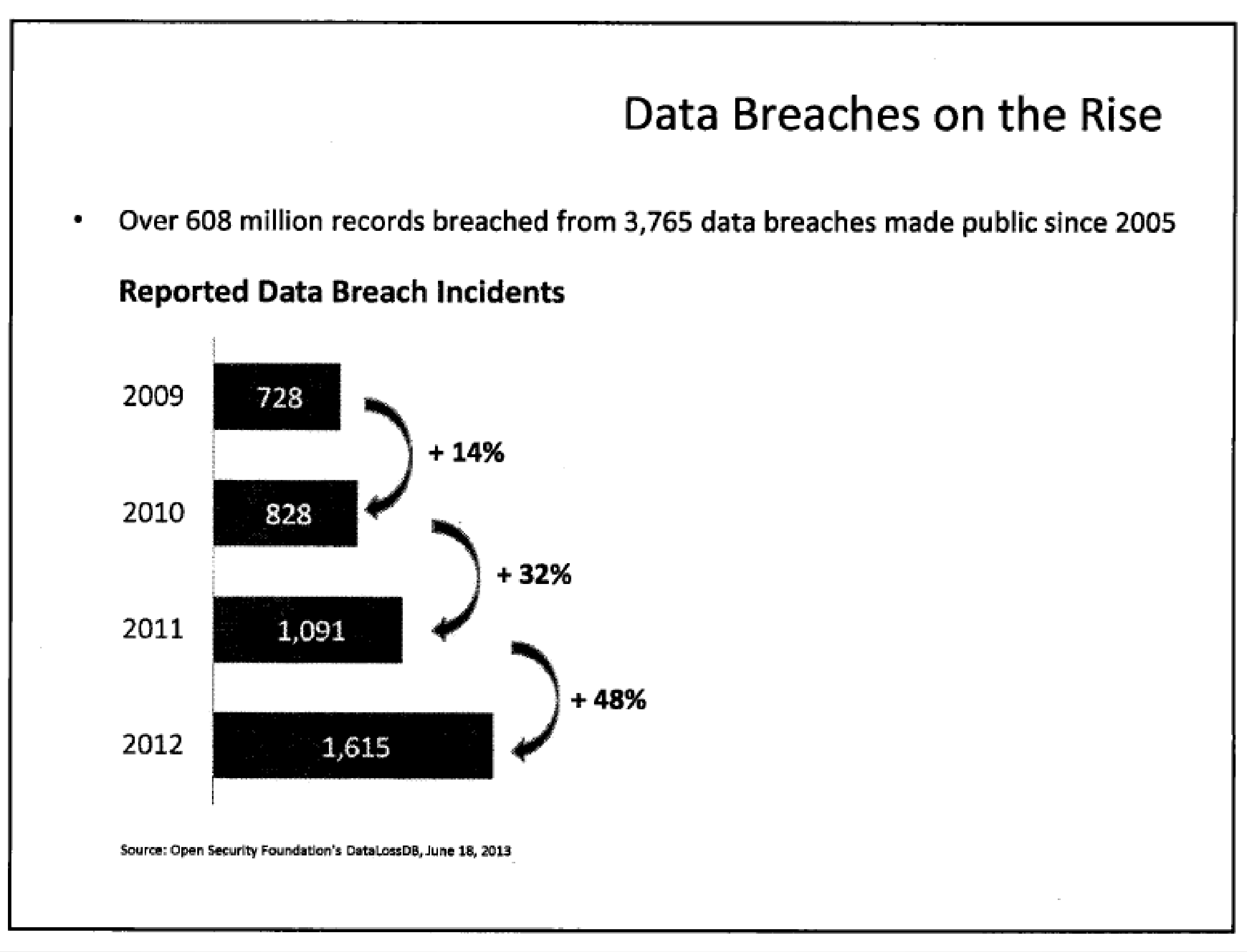
Identifying threats

- **Estimates of Target's probable losses**:
  - Avivah Litan, Gartner: **$420 million** (PCI fines, banks card-replacement costs, customer costs, legal fees, credit monitoring) (http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/);
  - Daniel Binder, Jeffries: **$400 million to $1.1 billion** (PCI fines and assessments) (theflyonthewall.com, 1/30/2014)
- **Estimated number of individuals who did not shop at Target** in early January due to the reported breach:
  - **7%** of pre-breach volume: **4.6 million shoppers** (http://www.forbes.com/sites/prospernow/2014/01/24/amazon-sets-the-standard-for-shopper-security-while-target-struggles/)

Identifying threats

- **Costs for 137 insurance claims** (2012 NetDiligence report):
  - Range: **$2k to $76 million**;
  - **Average costs per breach**: **$3.7 million total**
    - Average cost of **legal settlements: $2.1 million**
    - Average **legal fees for litigation: $582k**
    - Average **crisis services** (forensics, breach response counsel, credit monitoring): **$983k**

Identifying threats



Data Breaches on the Rise

- Over 608 million records breached from 3,765 data breaches made public since 2005

Reported Data Breach Incidents

Source: Open Security Foundation's DataLossDB, June 18, 2013

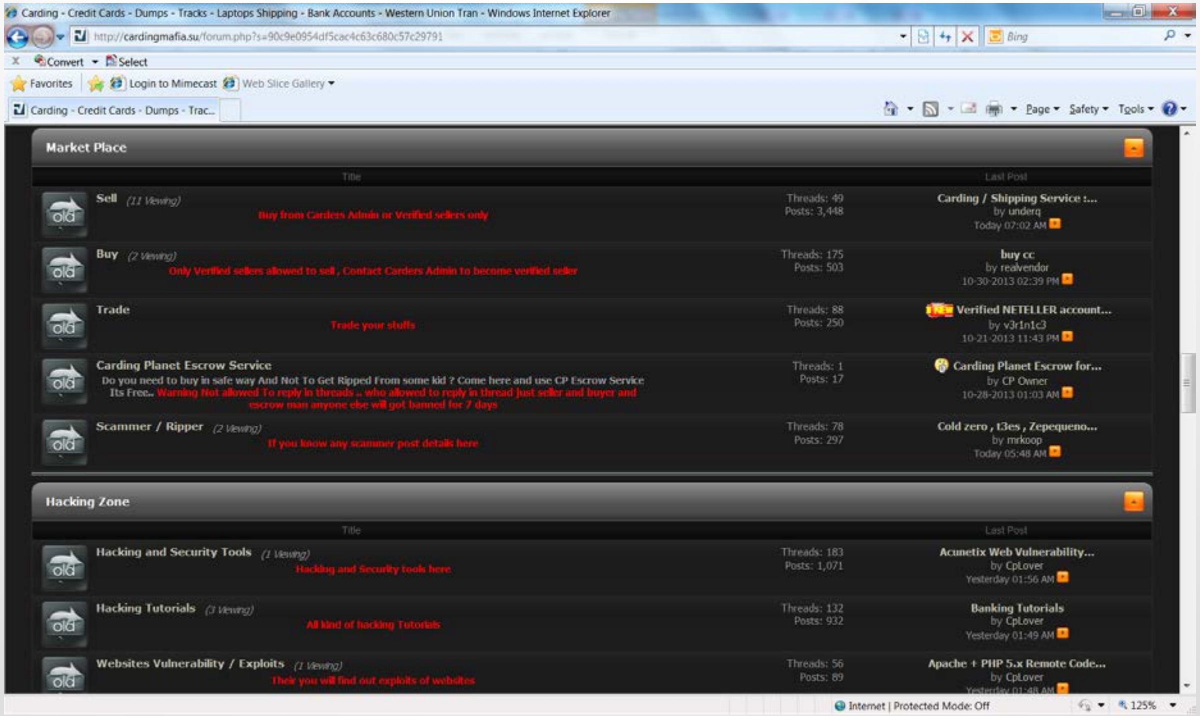
Evaluating Cyber Liability Insurance Policies, ABA Standing Committee on Professional Liability, Jan. 23, 2014, used with permission.

Identifying threats

- E. European and Russian **card thieves are well-organized**.
  - **Different groups specialize in**
    - **Creating and adapting malware**, such as the BlackPOS malware used in the Target, Nieman Marcus, and Michaels attacks;
    - **Implanting malware**;
    - **Exfiltrating card data**;
    - **Selling stolen card data**; and
    - **Running "mules"** to use cloned cards.

Identifying threats

- **Carder websites** openly sell stolen card data, offer samples of data to verify validity, and provide replacement card data for any data the buyer finds to be invalid.



Carding - Credit Cards - Dumps - Tracks - Laptops Shipping - Bank Accounts - Western Union Tran - Windows Internet Explorer

http://cardingmafia.su/forum.php?s=90c9e0954df5cac4c63c680c57c29791

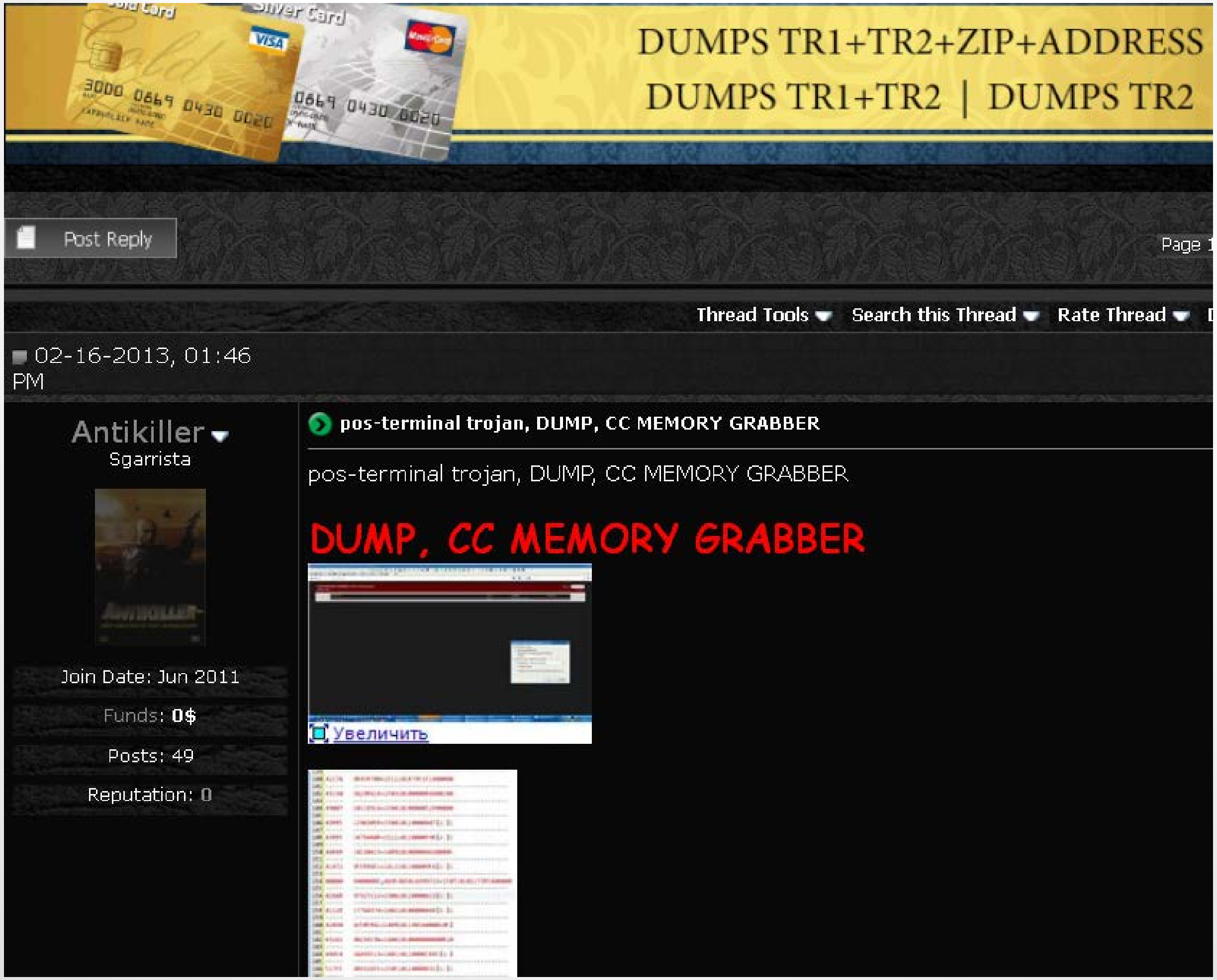
Market Place

Title		Last Post
Sell *(11 Viewing)* Buy from Carders Admin or Verified sellers only	Threads: 49 Posts: 3,448	**Carding / Shipping Service :...** by underq Today 07:02 AM
Buy *(2 Viewing)* Only Verified sellers allowed to sell , Contact Carders Admin to become verified seller	Threads: 175 Posts: 503	**buy cc** by realvendor 10-30-2013 02:39 PM
Trade Trade your stuffs	Threads: 88 Posts: 250	NEW **Verified NETELLER account...** by v3r1n1c3 10-21-2013 11:43 PM
Carding Planet Escrow Service Do you need to buy in safe way And Not To Get Ripped From some kid ? Come here and use CP Escrow Service Its Free.. Warning Not allowed To reply in threads .. who allowed to reply in thread just seller and buyer and escrow man anyone else will got banned for 7 days	Threads: 1 Posts: 17	**Carding Planet Escrow for...** by CP Owner 10-28-2013 01:03 AM
Scammer / Ripper *(2 Viewing)* If you know any scammer post details here	Threads: 78 Posts: 297	**Cold zero , t3es , Zepequeno...** by mrkoop Today 05:48 AM

Hacking Zone

Title		Last Post
Hacking and Security Tools *(1 Viewing)* Hacking and Security tools here	Threads: 183 Posts: 1,071	**Acunetix Web Vulnerability...** by CpLover Yesterday 01:56 AM
Hacking Tutorials *(3 Viewing)* All kind of hacking Tutorials	Threads: 132 Posts: 932	**Banking Tutorials** by CpLover Yesterday 01:49 AM
Websites Vulnerability / Exploits *(1 Viewing)* Their you will find out exploits of websites	Threads: 56 Posts: 89	**Apache + PHP 5.x Remote Code...** by CpLover Yesterday 01:48 AM

Identifying threats



02-16-2013, 01:46 PM

Antikiller
Sgarrista

Join Date: Jun 2011

Funds: **0$**

Posts: 49

Reputation: 0

pos-terminal trojan, DUMP, CC MEMORY GRABBER

pos-terminal trojan, DUMP, CC MEMORY GRABBER

DUMP, CC MEMORY GRABBER

http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/

Identifying threats

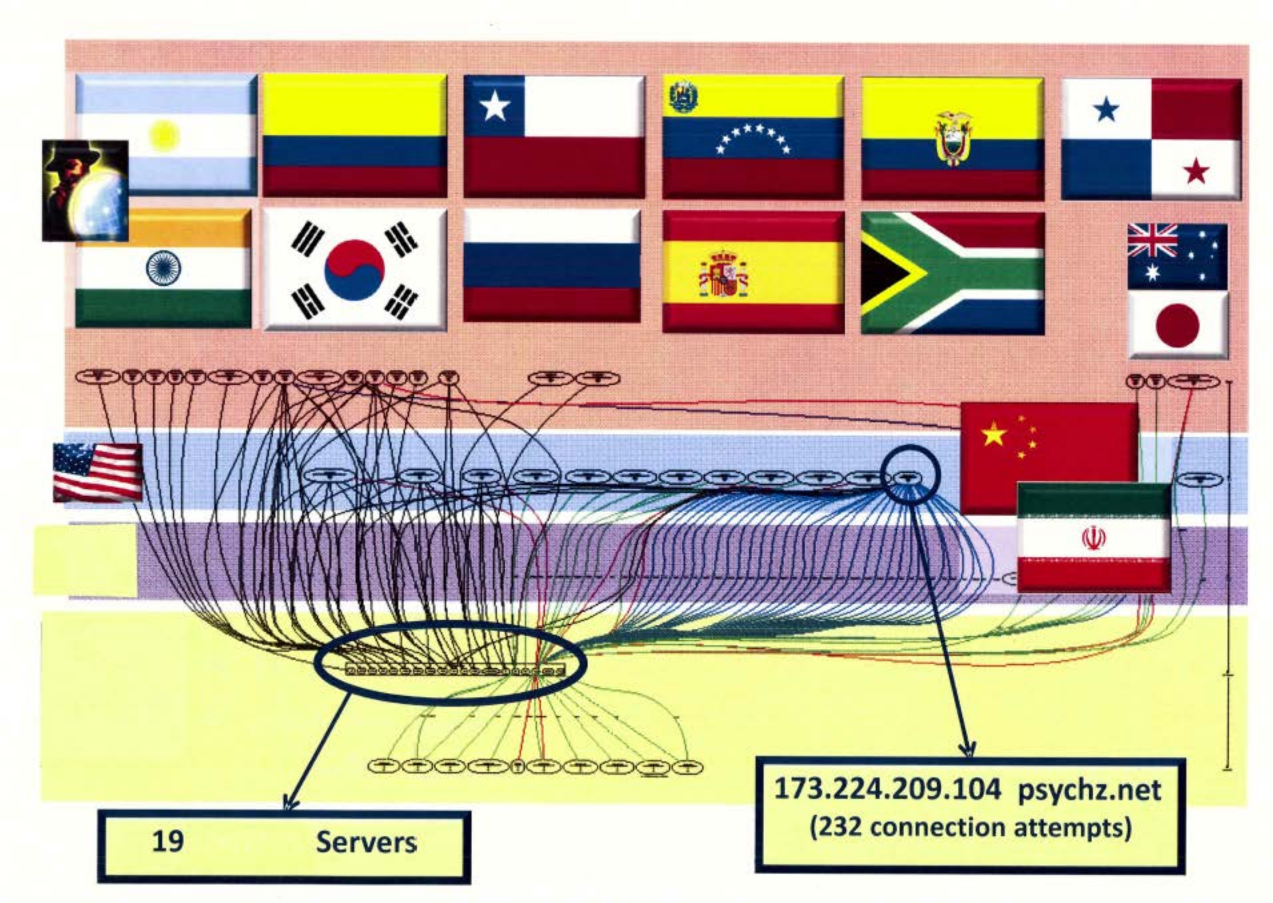
- The U.S. Department of Justice has indicted and prosecuted both U.S.-based and foreign hackers. E.g.,
  - **Albert Gonzalez**, a ring-leader in the Hannaford breach and many others, is **currently serving a 20-year sentence**.
  - **Four Russians and a Ukrainian were recently indicted for their roles in 14 different breaches in which 170.5 million payment card datasets** were stolen. *U.S. v. Drinkman, et al.*, Second Superseding Indictment, Cr. No. 09-626 (D. N.J. July 25, 2013).

Identifying threats

- If your business
  - is among those **identified for development in the Chinese 2011-2015 five-year plan** (new energy, energy conservation, biotechnology, rare earth materials and high-end semiconductors, information technology, aerospace and telecom equipment, and clean energy vehicles)
  - and it **creates or uses valuable intellectual property**,
- **State-sponsored attackers** are trying to steal the intellectual property. Mandiant, "APT1 - Exposing One of China's Cyber Espionage Units," 24 (Feb. 18, 2013), *available at* http://www.mandiant.com/apt1.
- **Cyber-espionage increased 42% in 2012** over 2011 (Christopher Versace, "Cyber Attacks," *Forbes*, June13, 2013).
- **31% of such attacks target businesses with fewer than 250 employees**. *Id.*

Identifying threats

- E.g., during a 24-hour period, one Wa. entity counted **4,000 attacks** from 16 countries on 19 of its 300,000 computers:



Identifying threats

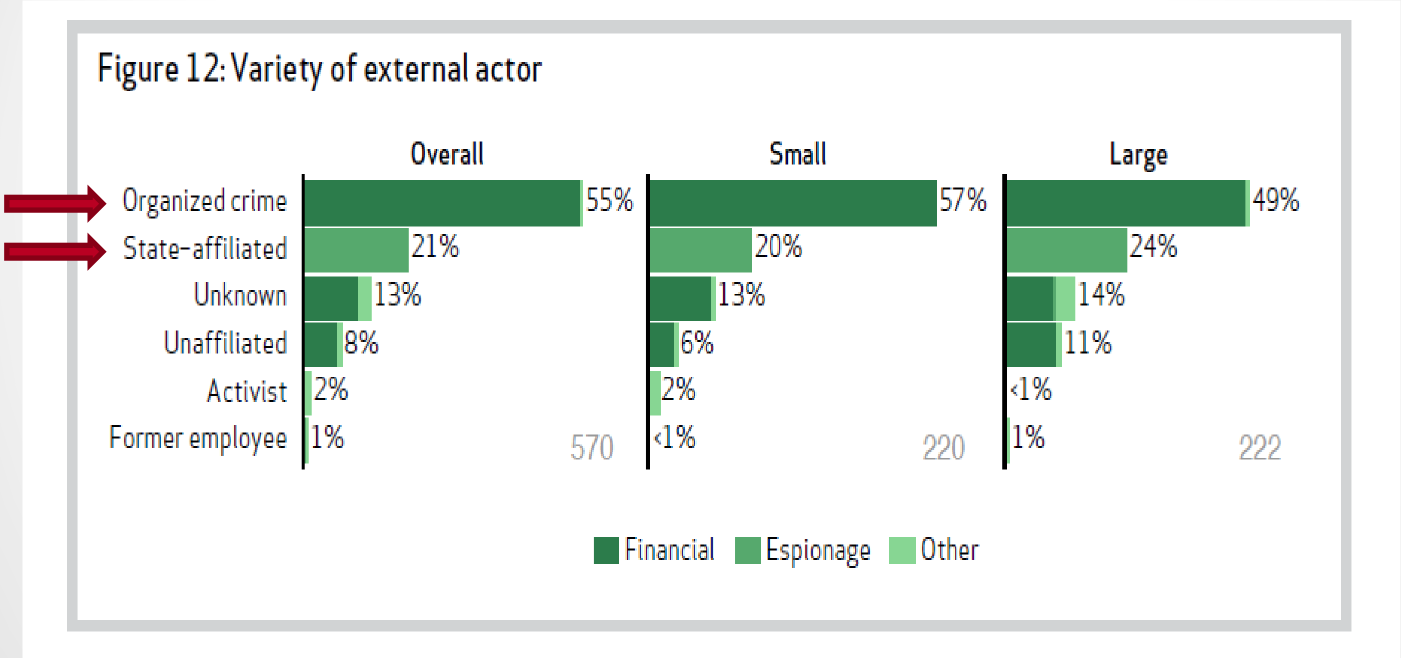


Figure 12: Variety of external actor

Verizon 2013 Data Breach Investigations Report, 21.

Identifying threats

- Richard Clarke, cybersecurity and cyber-terrorism advisor to Presidents Reagan, H.W. Bush, Clinton, George W. Bush, and Obama:
  - "**Every major company in the United States has already been penetrated by China**. **[W]e lose our competitiveness by having all of our research and development stolen by the Chinese**."

Emil Protalinski, "Richard Clarke: China has hacked every major US company," http://www.zdnet.com/blog/security (March 27, 2012).

Identifying threats

- U.S. Army Gen. Keith B. Alexander, Director of the National Security Agency:

  - The loss of industrial information and intellectual property through cyber espionage constitutes the "**greatest transfer of wealth in history**," estimated at **$250 billion per year**.

Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history,'" http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history (July 9, 2012).

Identifying threats

- "China stands out in regard to attacks for IP…. **Chinese businesses thrive on stolen technology**." *IP Commission Report*, 18 (May 2013)
- Verizon determined that **China was responsible for 96% of the "espionage" attacks** it encountered. 2013 Verizon Data Breach Incident Report, 21.
- "**[C]yber spying has been an indispensable accelerant for China's military** and economic rise." Stewart Baker, "The Attribution Revolution," *Foreign Policy* (June 17, 2013), http://www.foreignpolicy.com/articles/2013/06/17/the_attribution_revolution_plan_to_stop_cyber_attacks?page=full.

Identifying threats

- Mandiant identified a **Chinese PLA Unit 61398**, a/k/a the "Comment Crew," responsible for 141 thefts from U.S. and other businesses:

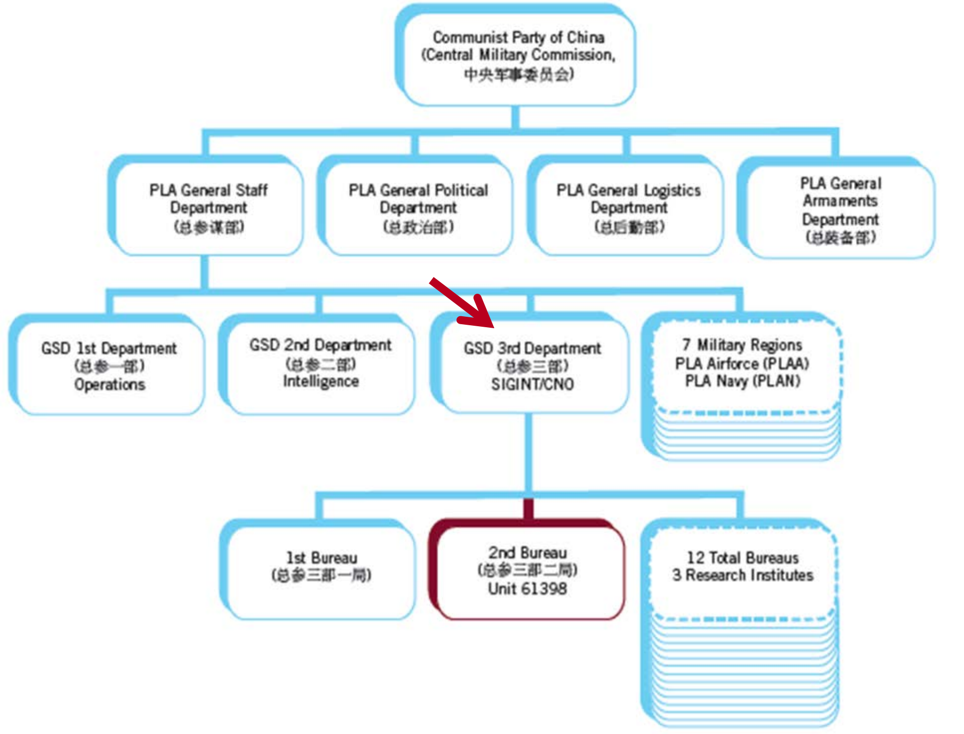

Communist Party of China (Central Military Commission, 中央军事委员会)
PLA General Staff Department (总参谋部)
PLA General Political Department (总政治部)
PLA General Logistics Department (总后勤部)
PLA General Armaments Department (总装备部)
GSD 1st Department (总参一部) Operations
GSD 2nd Department (总参二部) Intelligence
GSD 3rd Department (总参三部) SIGINT/CNO
7 Military Regions PLA Airforce (PLAA) PLA Navy (PLAN)
1st Bureau (总参三部一局)
2nd Bureau (总参三部二局) Unit 61398
12 Total Bureaus 3 Research Institutes

FIGURE 1: Unit 61398's position within the PLA[11]

Mandiant, "APT1 - Exposing One of China's Cyber Espionage Units," 8 (Feb. 18, 2013), *available at* http://www.mandiant.com/apt1.

Identifying threats

- PLA Unit 61398, a/k/a the 2d Bureau of **the 3d Department of the PLA General Staff Department**, focusses on "**signals intelligence**, foreign language proficiency, and **defense information systems**."

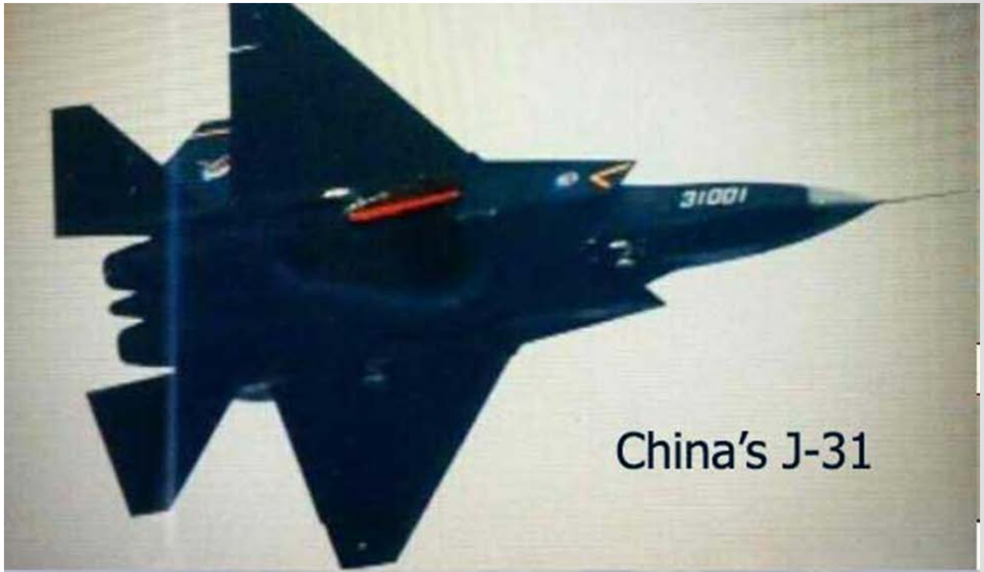
Mandiant, APT1 report at 7.

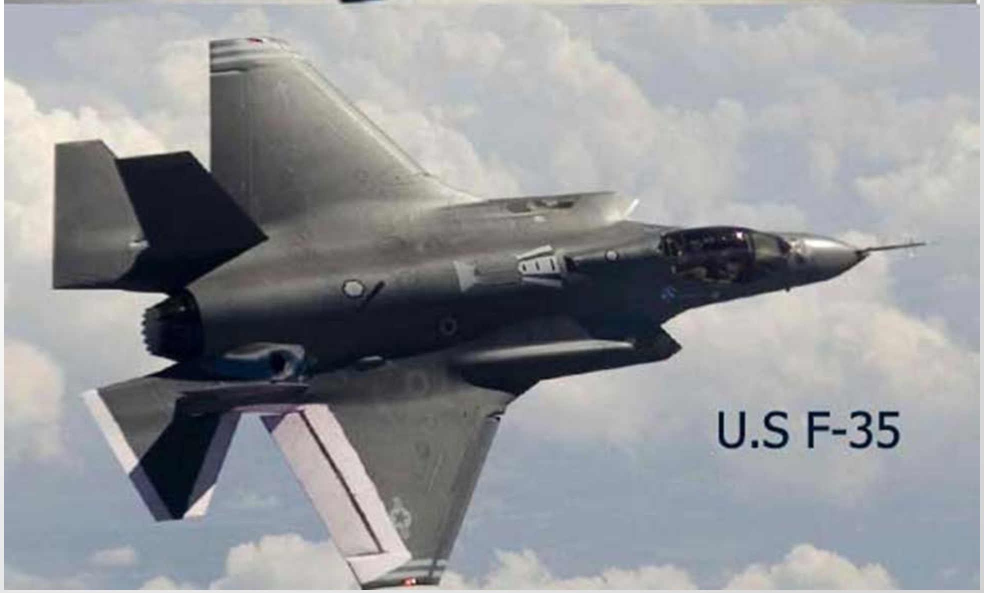
- "Operationally, **the PLA's Third Department is in the driving seat**: almost all serious exploitation operations are directed out of 3/PLA official premises. **The focus has increasingly been on penetrating core systems** …."

United States Naval War College and the University of California Institute on Global Conflict and Cooperation, *China and Cyber Security: Political, Economic, and Strategic Dimensions* (April 2012)

Identifying threats

- One result:





Photos courtesy of Gregory Fowler, Special Agent in Charge, FBI, Portland, OR

Identifying threats

- Mandiant provides both proactive threat assessments to determine if computer networks have been hacked and incident response services to locate and remove hacker tools from networks.
- Mandiant contact:
  - Chris Bream, Manager, chris.bream@mandiant.com, 703.224.2967.

Identifying threats

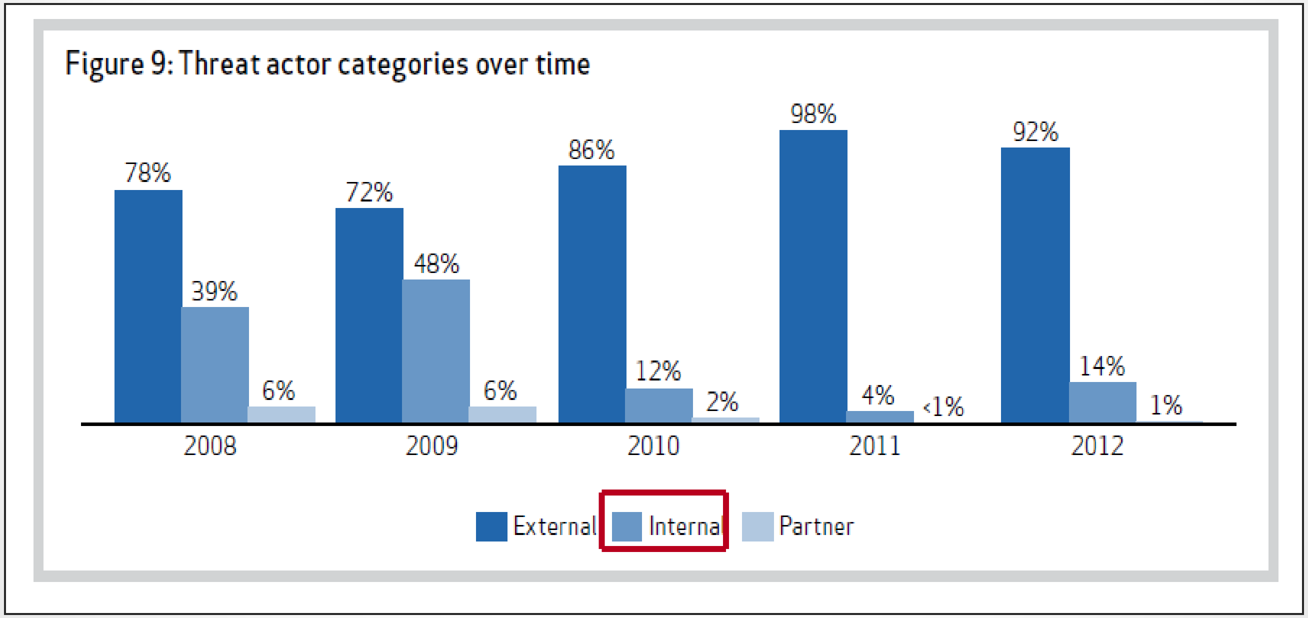


Figure 9: Threat actor categories over time

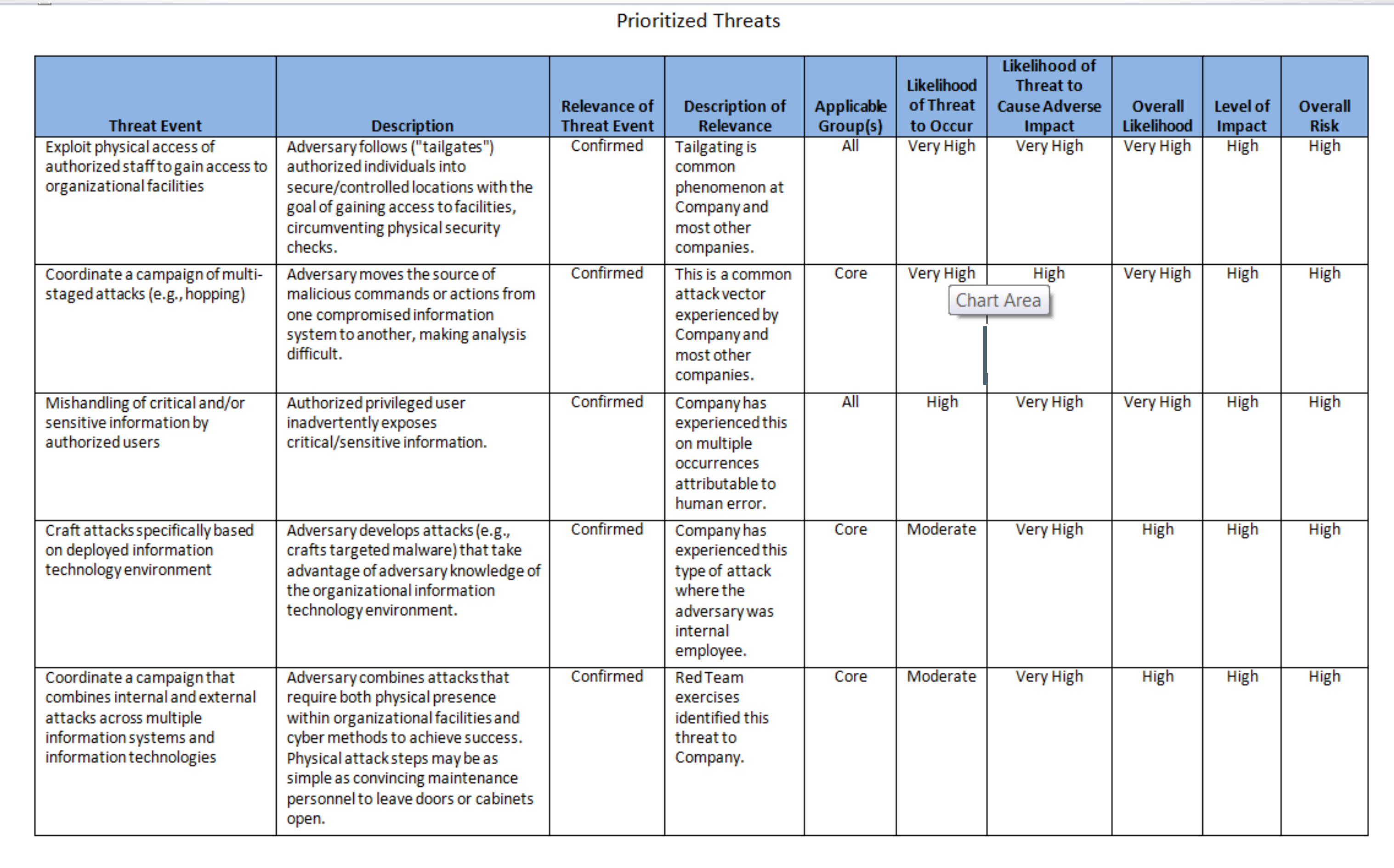
Verizon 2013 Data Breach Investigations Report, 19.

Identifying threats

- Employees and contractors also steal data:
  - Angry ex-employees;
  - ID thieves not blocked by background checks;
  - Problem employees.

Risk assessments can help

- A NIST SP 800-30 risk assessment:



Prioritized Threats

Threat Event	Description	Relevance of Threat Event	Description of Relevance	Applicable Group(s)	Likelihood of Threat to Occur	Likelihood of Threat to Cause Adverse Impact	Overall Likelihood	Level of Impact	Overall Risk
Exploit physical access of authorized staff to gain access to organizational facilities	Adversary follows ("tailgates") authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.	Confirmed	Tailgating is common phenomenon at Company and most other companies.	All	Very High	Very High	Very High	High	High
Coordinate a campaign of multi-staged attacks (e.g., hopping)	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.	Confirmed	This is a common attack vector experienced by Company and most other companies.	Core	Very High	High	Very High	High	High
Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.	Confirmed	Company has experienced this on multiple occurrences attributable to human error.	All	High	Very High	Very High	High	High
Craft attacks specifically based on deployed information technology environment	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.	Confirmed	Company has experienced this type of attack where the adversary was internal employee.	Core	Moderate	Very High	High	High	High
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies	Adversary combines attacks that require both physical presence within organizational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.	Confirmed	Red Team exercises identified this threat to Company.	Core	Moderate	Very High	High	High	High

Risk assessments can help

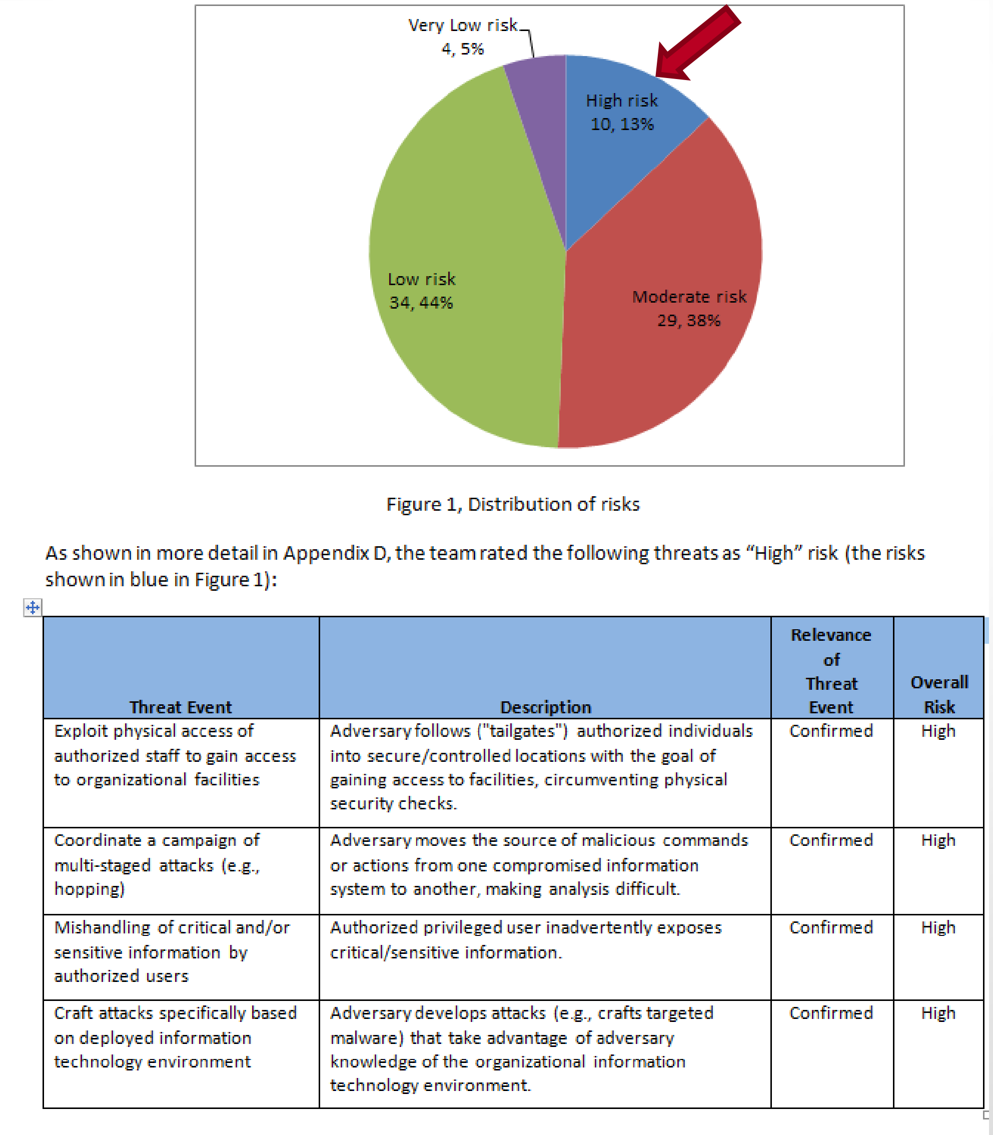

Very Low risk
4, 5%
High risk
10, 13%
Moderate risk
29, 38%
Low risk
34, 44%

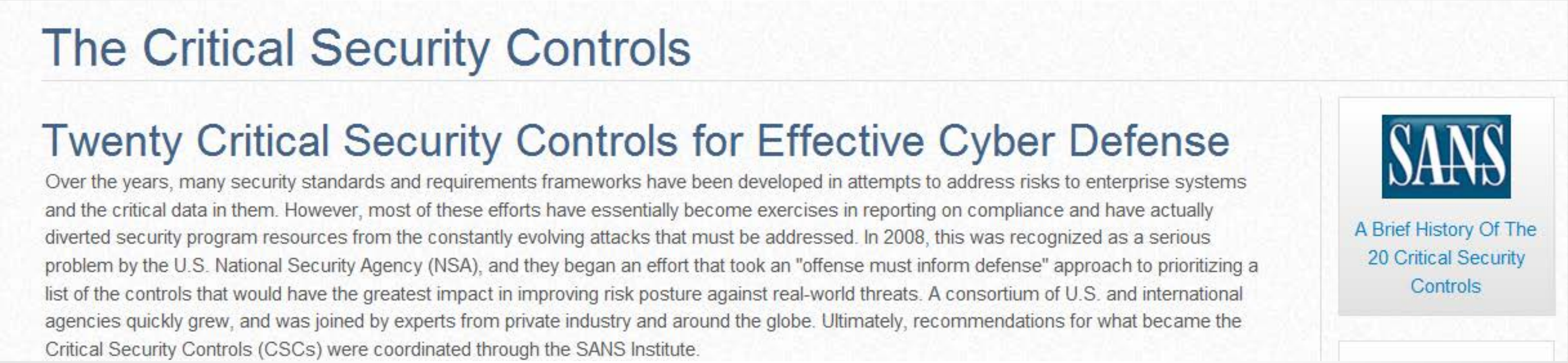
Figure 1, Distribution of risks

As shown in more detail in Appendix D, the team rated the following threats as “High” risk (the risks shown in blue in Figure 1):

Threat Event	Description	Relevance of Threat Event	Overall Risk
Exploit physical access of authorized staff to gain access to organizational facilities	Adversary follows ("tailgates") authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.	Confirmed	High
Coordinate a campaign of multi-staged attacks (e.g., hopping)	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.	Confirmed	High
Mishandling of critical and/or sensitive information by authorized users	Authorized privileged user inadvertently exposes critical/sensitive information.	Confirmed	High
Craft attacks specifically based on deployed information technology environment	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.	Confirmed	High

Risk assessments can help

- A SANS Critical Controls Gap Assessment:

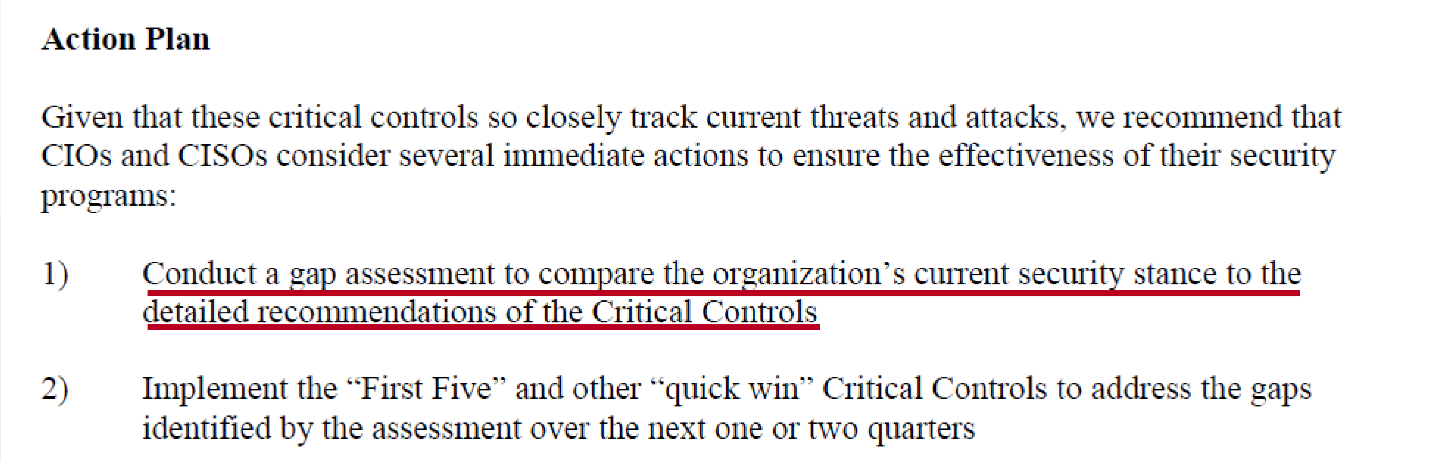


The Critical Security Controls

Twenty Critical Security Controls for Effective Cyber Defense

Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed. In 2008, this was recognized as a serious problem by the U.S. National Security Agency (NSA), and they began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats. A consortium of U.S. and international agencies quickly grew, and was joined by experts from private industry and around the globe. Ultimately, recommendations for what became the Critical Security Controls (CSCs) were coordinated through the SANS Institute.

A Brief History Of The 20 Critical Security Controls



Action Plan

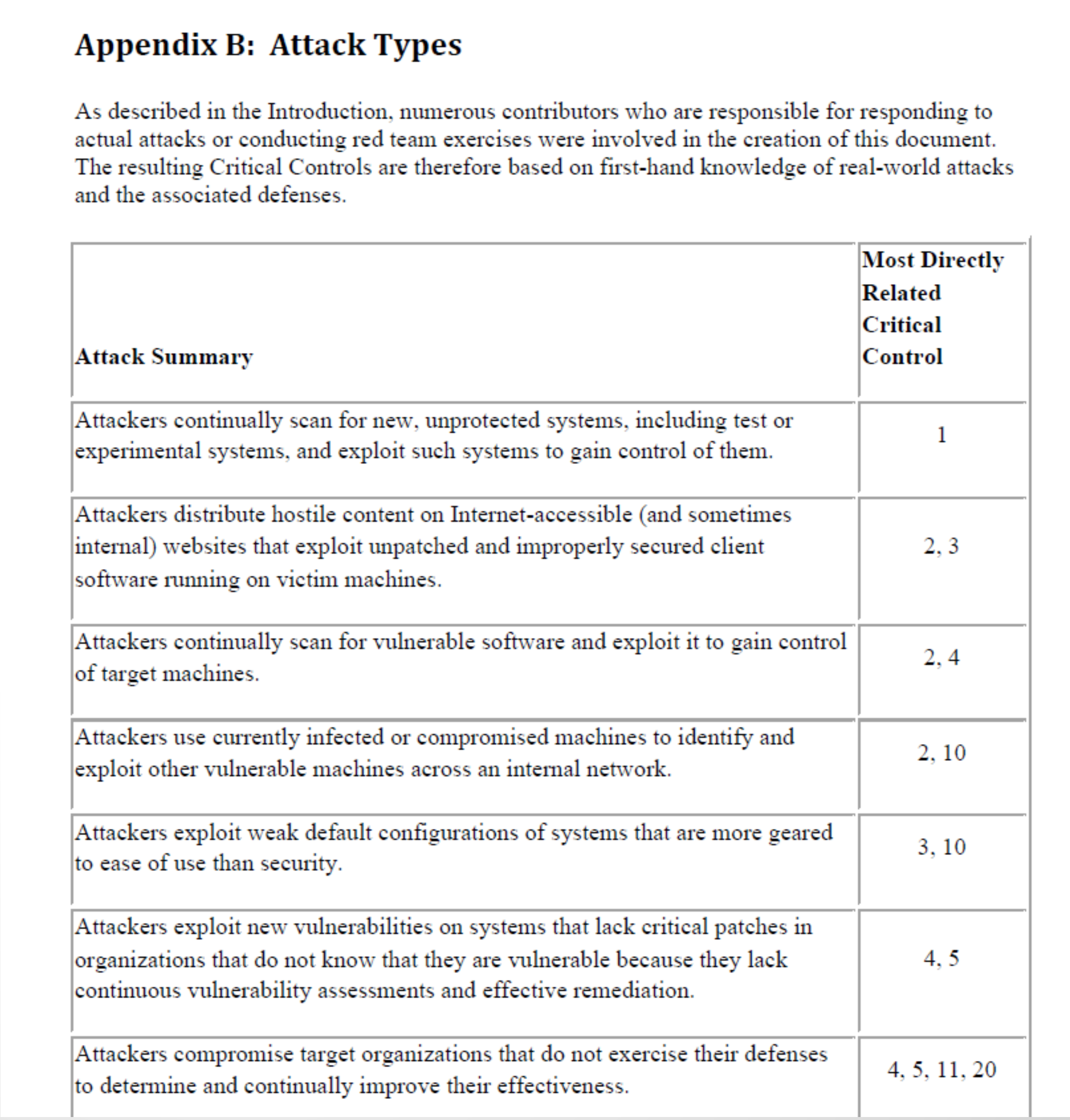
Given that these critical controls so closely track current threats and attacks, we recommend that CIOs and CISOs consider several immediate actions to ensure the effectiveness of their security programs:

1) Conduct a gap assessment to compare the organization's current security stance to the detailed recommendations of the Critical Controls

2) Implement the "First Five" and other "quick win" Critical Controls to address the gaps identified by the assessment over the next one or two quarters

Risk assessments can help

- Each require you to identify pertinent threats.
  - E.g., SANS Critical Security Controls, App. B.



Appendix B: Attack Types

As described in the Introduction, numerous contributors who are responsible for responding to actual attacks or conducting red team exercises were involved in the creation of this document. The resulting Critical Controls are therefore based on first-hand knowledge of real-world attacks and the associated defenses.

Attack Summary	**Most Directly Related Critical Control**
Attackers continually scan for new, unprotected systems, including test or experimental systems, and exploit such systems to gain control of them.	1
Attackers distribute hostile content on Internet-accessible (and sometimes internal) websites that exploit unpatched and improperly secured client software running on victim machines.	2, 3
Attackers continually scan for vulnerable software and exploit it to gain control of target machines.	2, 4
Attackers use currently infected or compromised machines to identify and exploit other vulnerable machines across an internal network.	2, 10
Attackers exploit weak default configurations of systems that are more geared to ease of use than security.	3, 10
Attackers exploit new vulnerabilities on systems that lack critical patches in organizations that do not know that they are vulnerable because they lack continuous vulnerability assessments and effective remediation.	4, 5
Attackers compromise target organizations that do not exercise their defenses to determine and continually improve their effectiveness.	4, 5, 11, 20

Risk assessments can help

- If the risk assessment is **conducted by** or at the direction of **counsel** and the **primary purpose** of the assessment is **to determine** the extent of the business's **potential liability** for lost or stolen data
  - The risk assessment report should be **protected** from discovery **by the attorney-client privilege**.

Risk assessments can help

- **If your data security measures are under-developed**:
  - Meet with a capable security consultant;
  - **Determine the first steps you should take** to secure your information; and
  - **Develop a plan** to implement appropriate data security measures.
- One consultant to consider:
  - Accuvant Labs, Luke Papineau, lukep@accuvant.com, 425.242.6518.

Cost-effective security measures

- **For compliance purposes**, ensure you have "appropriate" security measures as required by FTC consent orders:
  - Assign responsibility;
  - Identify information assets;
  - **Conduct risk assessments**;
  - Select and implement responsive security controls;
  - Monitor effectiveness;
  - Regularly review program; and
  - Address third party issues.

Thomas J. Smeddinghoff, "Data Security Requirements for Non-Regulated Business Sectors," *14th Annual Institute on Privacy and Data Security*, Vol. 2, Ch. 9 (May 2013)

Cost-effective security measures

- But beyond “compliance,” **what will get the job done?**
- And what’s “appropriate” when **firewalls, AVS, antimalware protection, endpoint protection and IDPS can be bypassed** by attacks that use customized malware?

Cost-effective security measures

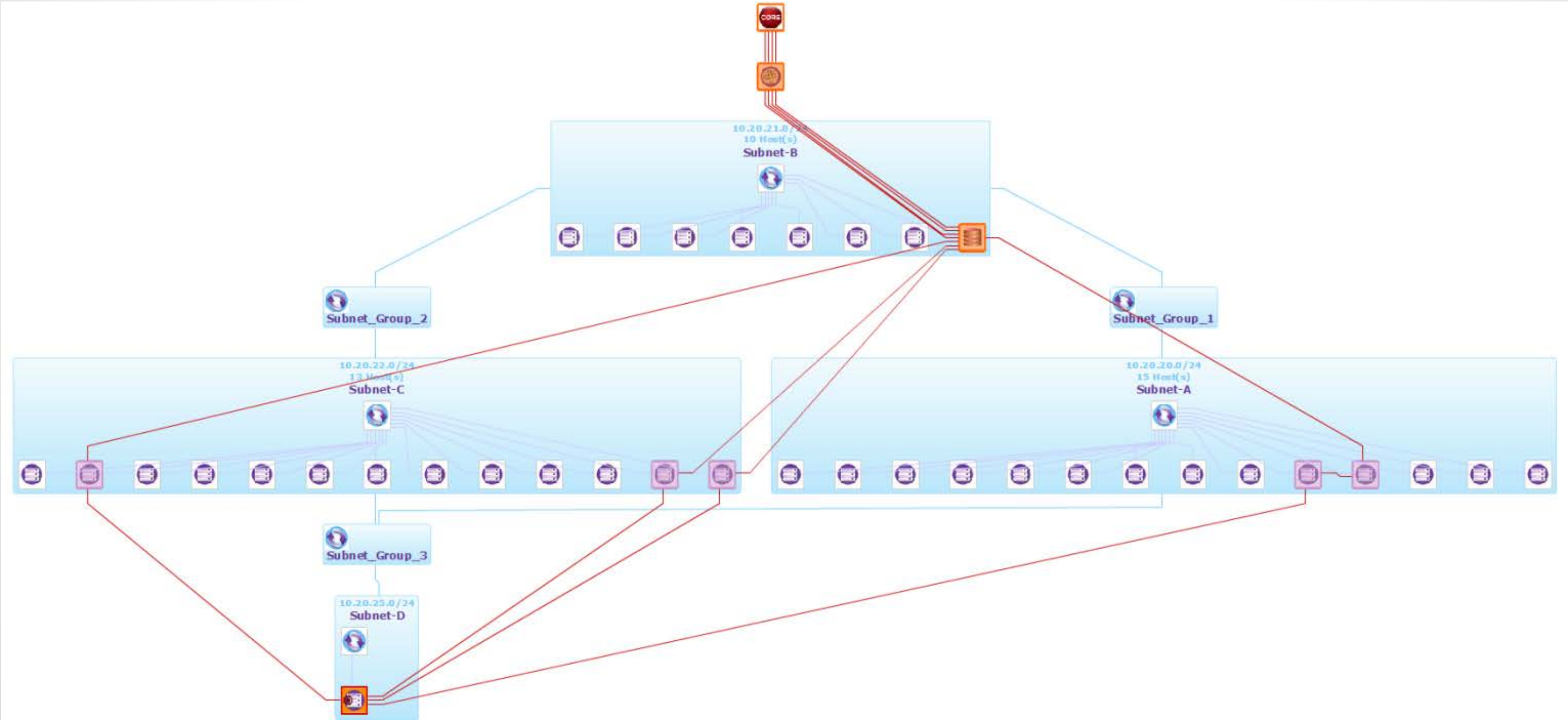
- One large organization's network defense strategy:
  - There is **no perimeter**
  - **Assume breach**
  - **Use situational awareness**
  - **Use layered defenses to protect high-value assets.**

Cost-effective security measures

- **Use situational awareness, unlike our friend here:**

Cost-effective security measures

- Sophisticated penetration tests and vulnerability scans can identify holes you need to fix.



CORE SECURITY Thinking ahead Insight Enterprise Intelligence tool. Used with permission.

Cost-effective security measures

- Core Security
  - Eric Cowperthwaite, ecowperthwaite@coresecurity.com, 206.409.4036

Cost-effective security measures

- Basic measures must still be maintained, e.g.,
  - **Implement** administrative, physical, and technical **safeguards** no less rigorous than those required by industry standards, including
    - **ISO-IEC 27001**:2005 and **ISO-IEC 27002**:2005;
    - The **HIPAA Security Rule** for businesses to which the Rule applies;
    - **PCI DSS 3.0** for payment card data; and
    - **GLB requirements** for federally regulated financial entities.

Cost-effective security measures

- At a minimum:
  - **limit access to** confidential information **to authorized persons who need access**;
  - **physically secure** business **facilities**, data centers, paper files, servers, back-up systems, and computing equipment;
  - **implement authentication and access controls**;
  - **encrypt confidential information** stored on mobile devices and media and transmitted over public or wireless networks;
  - **segregate sensitive information** and provide additional safeguards;
  - implement appropriate personnel security practices, including **conducting background checks**; and
  - **provide privacy and security training to employees**.

Cost-effective security measures

- Data **encryption** is important but, depending on how it’s deployed, will not stop some attacks:
  - Alleged **Global Payments** hacker:
    - “They finished End2End encryption, but E2E not a full solution; it only defend [sic] from outside threat.”
  - **The alleged hacker claimed he and his colleagues had been in Global Payments’ system for 13 months, collecting data monthly**.

Brian Krebs, *Global Payments: Rumor and Innuendo*, (April 2, 2012), http://krebsonsecurity.com/2012/04/global-payments-rumor-and-innuendo/.

Cost-effective security measures

- **Data Loss Prevention tools** can help **block** employees and others from **exfiltrating confidential data**.
- Employee **training**, coupled with **tools that monitor employee activity on business networks**, can also help stop careless, uninformed , and malicious employees from disclosing sensitive data.

Cost-effective security measures

- **Ensure the software you run does not have common security flaws** such as those listed in
  - the CWE/SANS Top 25 Programming Errors

    http://cwe.mitre.org/top25/ or http://www.sans.org/top25-programming-errors/

    and
  - the Open Web Application Security Project's (OWASP) Top Ten Project

    https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Cost-effective security measures

- But to counter APT attacks, you need tools that
  - Don’t rely on signatures;
  - Detect exploits; and
  - Provide actionable intel.

Jan Coulson, “Why Our Risk Assessment Calculations Leave Us Exposed to APTs,” *FireEye Blog* (Oct. 30, 2013).

Cost-effective security measures

- Technologies that may serve as part of a layered security program :
  - Firewalls/**next-gen**eration **firewalls**;
  - Intrusion prevention/detection systems (**IPS/IDS**);
  - **UTMs** (firewall, IPS, anti-malware, Web filtering, etc.);
  - **Endpoint protection** suites (anti-malware, host firewalling, filtering);
  - Message hygiene filters;
  - Web hygiene filters;
  - **Network access control** (NAC);
  - Data loss prevention;
  - Security information and event management (**SIEM**)/log aggregation;
  - Network **vulnerability scanners**/Web app scanners;
  - Policy and **configuration management**;
  - **Patching** and software delivery;
  - **Web application firewalls**/database monitors;
  - **Penetration testing tools**; and
  - **Strong authentication**.

Diana Kelley, "Threat prevention techniques: Best practices for Threat Management," *Information Security Magazine* (Sept. 22, 2012).

Cost-effective security measures

- Security information and event management (**SIEM) systems can help** detect attacks **if**
  - **Multiple data sources are collected** (network, security, and server logs, identity data, networks flows, vulnerability scan results, configuration data);
  - Likely **threats are** modeled, **run against target data,** SIEM **rules are refined**, thresholds are optimized; and
  - **The process is regularly repeated**.

Mike Rothman, “SIEM Practices for advanced threat detection,” *SearchSecurity* (May 8, 2013)

Cost-effective security measures

- Consider adding **sandboxing**:
  - Using network traffic analysis to identify potential malware threats and
  - Examining the files in a segregated, virtual machine environment to determine which are malicious.

Cost-effective security measures

- **Attackers must succeed at all steps of the "kill chain,"** including
  - **Reconnaissance**, delivering and **installing malware**, **exploiting weaknesses** in network defenses, **communicating with C2 servers**, and **exfiltrating data**.
- **Make the attacker's job more difficult** and more expensive at every step.

Cost-effective security measures

- **Train users** to recognize socially engineered attempts to get them to open email attachments or click on links to poisoned websites.
- Regularly **test users** on how well they’re following anti-phishing rules.
- **Discipline users who refuse to learn**.

Cost-effective security measures

- The **SANS Critical Security Controls for Effective Cyber Defense** describe a step-by-step, prioritized deployment of these and other layered defenses.
- The **20 SANS Critical Security Controls** are:
  - 1: **Inventory** of Authorized and Unauthorized **Devices**
  - 2: **Inventory** of Authorized and Unauthorized **Software**
  - 3: **Secure Configurations** for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
  - 4: **Continuous Vulnerability Assessment and Remediation**
  - 5: **Malware Defenses**
  - 6: **Application Software Security**

Cost-effective security measures

- 7: **Wireless Device Control**
- 8: **Data Recovery Capability**
- 9: **Security Skills Assessment** and Appropriate Training to Fill Gaps
- 10: **Secure Configurations for Network Devices** such as Firewalls, Routers, and Switches
- 11: **Limitation and Control of Network Ports**, Protocols, and Services
- 12: **Controlled Use of Administrative Privileges**
- 13: **Boundary Defense**
- 14: Maintenance, Monitoring, and **Analysis of Audit Logs**
- 15: Controlled **Access Based on the Need to Know**
- 16: **Account Monitoring and Control**
- 17: **Data Loss Prevention**
- 18: **Incident Response and Management**
- 19: **Secure Network Engineering**
- 20: **Penetration Tests and Red Team Exercises**

See http://www.sans.org/critical-security-controls/, v.4.1, p.1 (March 2013).

Cost-effective security measures

- The SANS Critical Security Controls were developed by experts from
  - NSA
  - NIST
  - DoD
  - Department of Energy Nuclear Laboratories
  - Department of Homeland Security Computer Emergency Readiness Team (CERT)
  - United Kingdom's Centre for the Protection of Critical Infrastructure
  - FBI and other law enforcement agencies
  - Australian Defence Signals Directorate and
  - Government and civilian penetration testers and incident handlers.

Id. at 2-3.

Cost-effective security measures

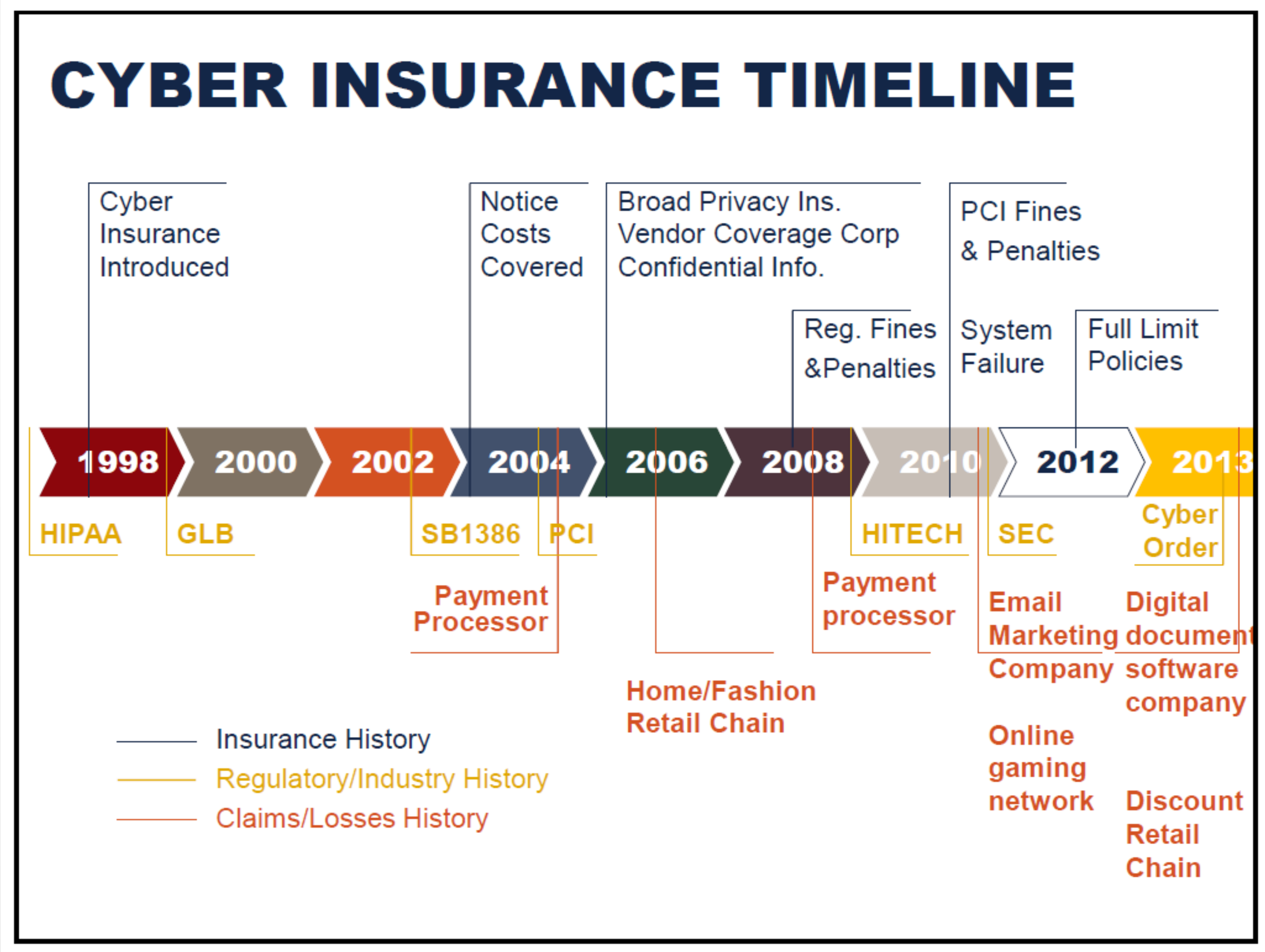
- The Consortium of Cybersecurity Action, which maintains the Controls, notes a pattern of steps organizations have taken to effectively implement the Controls:
  - 1. **Perform an Initial Gap Assessment** – determining what has been implemented and where gaps remain for each control and sub-control.
  - 2. **Develop an Implementation Roadmap** – selecting the specific controls (and sub-controls) to be implemented in each phase, and scheduling the phases based on business risk considerations.
  - 3. **Implement the First Phase of Controls** – identifying existing tools that can be repurposed or more fully utilized, new tools to acquire, processes to be enhanced, and skills to be developed through training.
  - 4. **Integrate Controls into Operations** – focusing on continuous monitoring and mitigation and weaving new processes into standard acquisition and systems management operations.
  - 5. **Report and Manage Progress** against the Implementation Roadmap developed in Step 2. Then **repeat Steps 3-5** in the next phase of the Roadmap.

Id. at 4.

Cost-effective security measures

- The SANS Critical Security Controls "**focus on automation** to provide cost efficiency, measurable results, scalability, and reliability." *Id.* at 3.
- The SANS site lists **vendors who offer tools to help implement the Controls**. *See* http://www.sans.org/critical-security-controls/vendor-solutions.

Evaluating cyber insurance

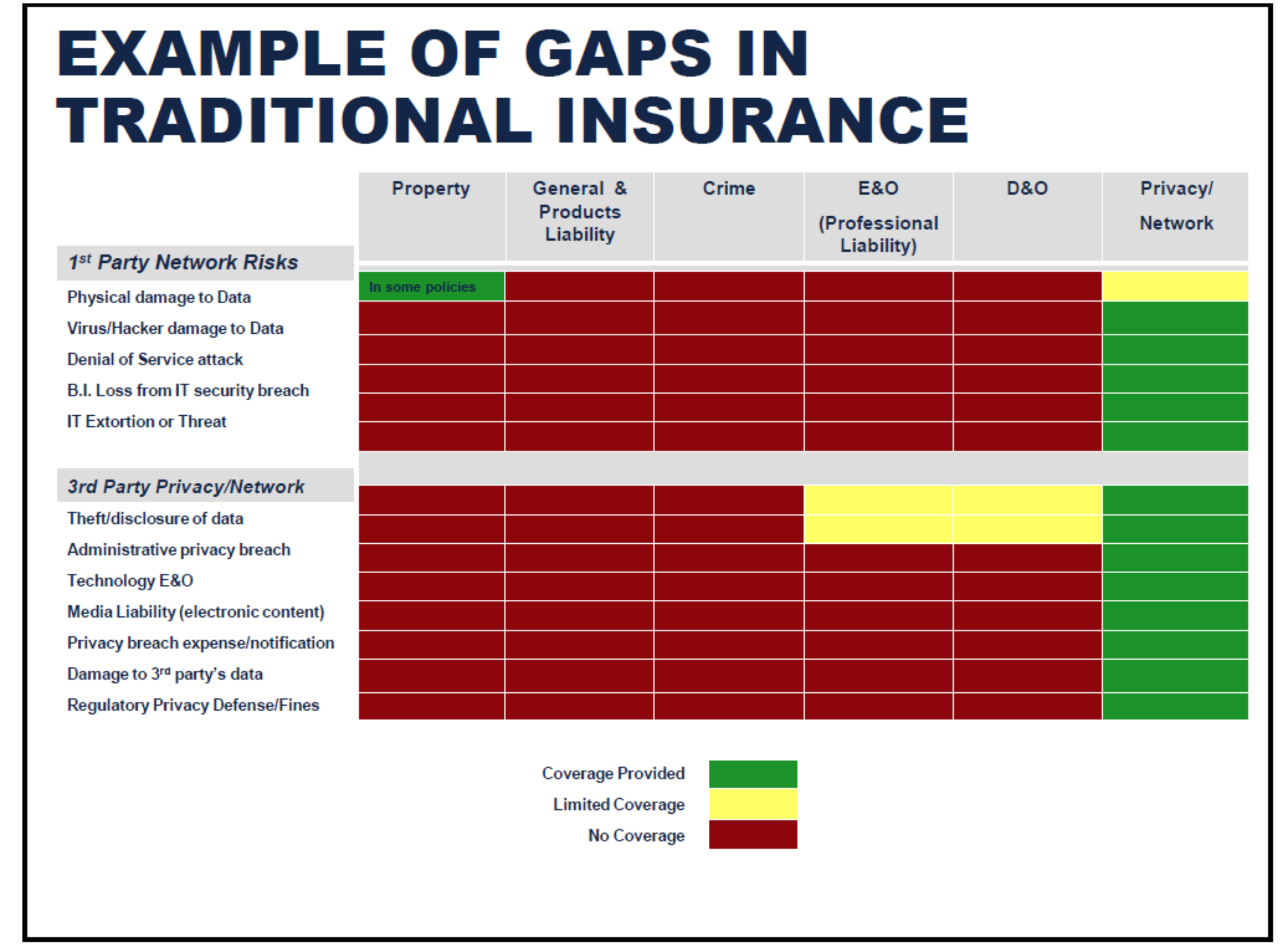


Evaluating Cyber Liability Insurance Policies, ABA Standing Committee on Professional Liability, Jan. 23, 2014, used with permission.

Evaluating cyber insurance

- **Gaps** in traditional insurance coverage:
  - **Intentional acts excluded** (GL)
  - **Data is not tangible** property (GL, Prop., Crime)
  - **Property damage required** to trigger (GL)
  - Theft or disclosure of **intellectual property and 3d-party info. often excluded** (GL)
  - **External hosting losses excluded** (GL)
  - **Only money, securities, tangibles covered** (Crime)
  - Coverage **restricted to acts U.S.**
  - **Sublimits or long wait periods for losses related to viruses** (Prop.)

Evaluating cyber insurance



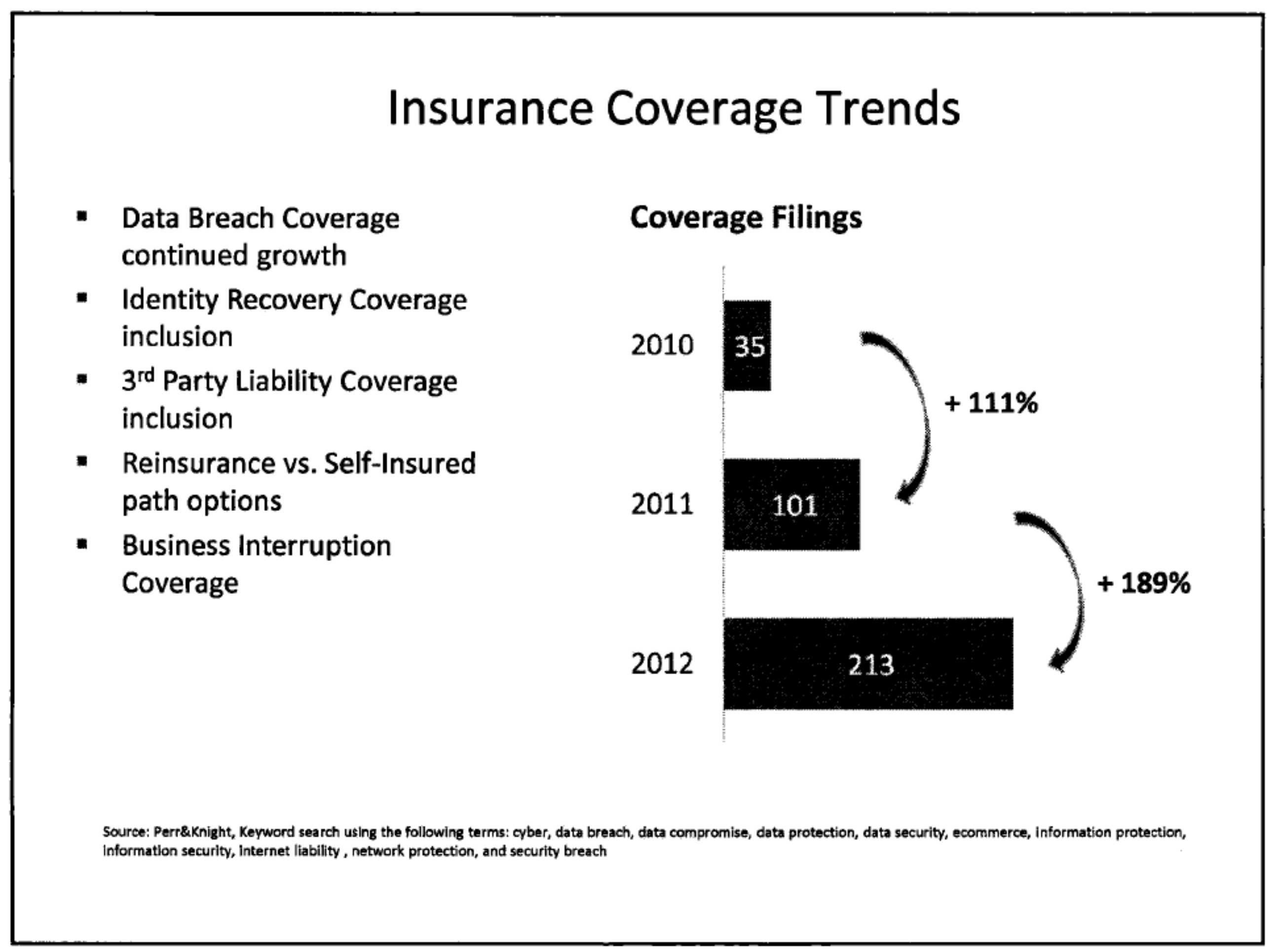
EXAMPLE OF GAPS IN TRADITIONAL INSURANCE

	Property	General & Products Liability	Crime	E&O (Professional Liability)	D&O	Privacy/ Network
1st Party Network Risks						
Physical damage to Data	🟩 In some policies	🟥	🟥	🟥	🟥	🟨
Virus/Hacker damage to Data	🟥	🟥	🟥	🟥	🟥	🟩
Denial of Service attack	🟥	🟥	🟥	🟥	🟥	🟩
B.I. Loss from IT security breach	🟥	🟥	🟥	🟥	🟥	🟩
IT Extortion or Threat	🟥	🟥	🟥	🟥	🟥	🟩
3rd Party Privacy/Network						
Theft/disclosure of data	🟥	🟥	🟥	🟨	🟨	🟩
Administrative privacy breach	🟥	🟥	🟥	🟨	🟨	🟩
Technology E&O	🟥	🟥	🟥	🟥	🟥	🟩
Media Liability (electronic content)	🟥	🟥	🟥	🟥	🟥	🟩
Privacy breach expense/notification	🟥	🟥	🟥	🟥	🟥	🟩
Damage to 3rd party's data	🟥	🟥	🟥	🟥	🟥	🟩
Regulatory Privacy Defense/Fines	🟥	🟥	🟥	🟥	🟥	🟩

Coverage Provided	🟩
Limited Coverage	🟨
No Coverage	🟥

Evaluating Cyber Liability Insurance Policies, ABA Standing Committee on Professional Liability, Jan. 23, 2014, used with permission.

Evaluating cyber insurance



Insurance Coverage Trends

- Data Breach Coverage continued growth
- Identity Recovery Coverage inclusion
- 3rd Party Liability Coverage inclusion
- Reinsurance vs. Self-Insured path options
- Business Interruption Coverage

Source: Perr&Knight, Keyword search using the following terms: cyber, data breach, data compromise, data protection, data security, ecommerce, information protection, information security, internet liability , network protection, and security breach

Id.

Evaluating cyber insurance

- Cyber insurance coverage to consider:
  - First party:
    - **Crisis management**
    - **Forensics**
    - **Business interruption**
    - **Remediation** (notifications, credit monitoring)
    - **Litigation defense**
    - **PCI fines and assessments**
    - **Regulatory fines and penalties**
    - **Extortion costs**
  - Third Party
    - "Privacy and Security," "Media Liability"

Evaluating cyber insurance

- **Exclusions** to watch for:
  - **Unencrypted data** on portable devices;
  - **Data not on insured’s system** (cloud, others);
  - **“Wild virus”** exclusion;
  - **Failure to maintain** system or update software;
  - **Short notice** requirements;
  - Exclusion of **employee data**;
  - Prior acts insured “**should have foreseen**”; and
  - **Physically stolen files** excluded.

Evaluating cyber insurance

- **Limits** to watch for:
  - **Narrow definition of “personal information**”;
  - **U.S.** privacy **statutes and regulations only**;
  - Coverage **limited by territory where cost incurred**;
  - **Voluntary costs excluded** (coverage triggered by legal liability);
  - **Requirements to use specific vendors**, counsel;
  - Inadequate **sublimit for forensics**;
  - Inadequate **sublimit for business interruption**;
  - **Sublimit for number of records**;
  - Deductibles, retentions, **limits tied to “incident**,” and
  - **Restricted right to settle**.

Evaluating cyber insurance

- **Enhancements** to consider:
  - **Choice of counsel**
  - **Prior acts**
  - **One retention** for entire policy
  - 1st party **coverage for insured's negligence** that causes system interruption
  - Limit intentional acts exclusion to control group to **ensure rogue employee acts are covered**
  - Ensure terrorism and "acts of war" exclusions **do not exclude state-sponsored thefts**

Evaluating cyber insurance

- **Factors that affect costs** of coverage:
  - Industry, loss record, **revenue**, likelihood of loss, number of records, number of employees, geography.
- **How much coverage is enough**?
  - Benchmark to peer data for claims, considering
    - Type of records (PCI, PHI, PII, IP), number of records, company’s public profile.

Evaluating cyber insurance

- A broker to consider:
  - Mark Ganley, Principal, AHT Insurance, Mganley@ahtins.com, 206.770.7948.

- **Questions?**

Randy Gainer, Attorney, CISSP
Davis Wright Tremaine LLP | Seattle
(206) 757-8047
email: randygainer@dwt.com