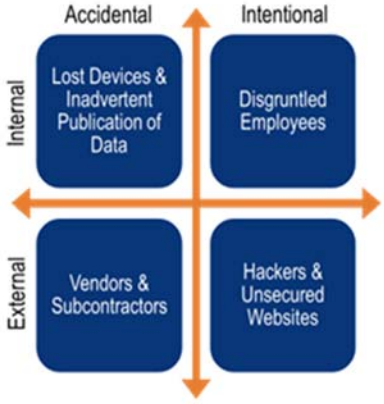
NAVIGANT

Information Security Newsletter – February 2015

2015 Information Security Predictions



- Increased Open Source Code Attacks (Example: Drupal)
- Undetectable/Cleaning Malware Continues To Proliferate
- Criminals Dissecting Security Tools and Posing as Debuggers
- Software / Website Development Companies Infiltrated for Weaknesses & Customer Lists
- Property Damage Caused by Cyber Attacks (German Iron Forge)
- Criminals Concentrating on Industries / Sectors When Successful (Parking Garages)
- Increased Insider Treats (Sony Pictures) and Disgruntled Employees (Morgan Stanley)
- Ransomware Evolving (CryptoWall) and Ransoms Increasing (Banque Cantonale de Geneve)

2014 Highlights

- ❖ 2014 had several huge breaches - Home Depot (56M), Target (70M), JPMorgan (83M) and eBay (145M).
- ❖ 1 Billion records or more were compromised in 2014 (Source: Forbes)

SPOTLIGHT ON MALWARE: BACKOFF AND NEW ENTRANTS

The use of malware in attacks against retailers Point of Sale (POS) systems in 2014 made headlines with disclosed breaches at Dairy Queen, Home Depot, UPS and Target to name a few. One type of malware that has targeted retailers is the Backoff strain. This malware, initially discovered in October 2013, has infected, according to a recent Secret Service bulletin, over 1,000 businesses. Backoff malware, in real terms, can scrape memory or search for credit card data, both track 1 and 2, from a POS terminal or system. The Command and Control (C2) component of Backoff can then upload discovered data as well as upload/download additional malware. Other recent Backoff upgrades and related malware identified include:

- ❖ ROM: The latest Backoff variant has several notable upgrades including disguising itself as a media player executable file and hashing the blacklist processes which undermines the ability to locate this malware.
- ❖ Spark: Spark, a variant of the Alina malware family, exploits a hole in the PCI-DSS retail security specifications. Spark is implanted into the memory of a POS system through an AutoIt script. Spark can copy and then transmit credit card data from a breached POS system.

Data Breach Legal / Legislative Update

- ❖ U.S. District Court Judge John W. Darrah dismissed a class action complaint filed against P.F. Chang's tied to a data breach in 2014. According to news reports, this ruling could carry implications for the, yet to be ruled on, motion to dismiss pleadings involving the ongoing consumer class action against Target.
- ❖ Governor Chris Christie signed into law on January 9, 2015, S562, which requires health insurance carriers that issue health benefit plans in New Jersey to encrypt personal information. New Jersey, according to news reports, is now the third state to require a higher level of encryption than HIPAA. This new law mandates security measures that implement safeguards that render the patient's data unreadable or unusable by someone who can bypass the password protection.
- ❖ California passed several new breach laws taking effect January 1, 2015 dealing with data breaches (AB 1710); medical information (AB1710) and students' (minors) personal information (AB 1755, AB1584 and SB1177).
- ❖ Benjamin Lawsky, Superintendent of the New York Department of Financial Services issued a letter to all financial institutions outlining a new cyber security assessment requiring answers on data protection as well as incident detection and response issues. The assessment is part of the examination process required for all New York state chartered banks.

NAVIGANT

SPOTLIGHT ON A NOTABLE DATA

Anthem, one of the nation's largest health insurers, disclosed hackers broke into company servers and gained access to information on as many as 80 million people. The company discovered the breach on January 29, 2015 and immediately alerted the FBI. The breached servers contained personal information on current and former customers as well as employees including names, Social Security numbers, birthdays, addresses, e-mail and employment information. The company believes the information compromised does include medical or credit card data. The hack is thought to be the largest breach involving a health care company in U.S. history. The company, in response to this breach, set up a dedicated website and toll-free number as well as free identity repair and credit monitoring services. According to news reports, the breach is suspected to be the work of Chinese hackers whose "fingerprint" fits the pattern of a group called Deep Panda.

ABOUT NAVIGANT'S INFORMATION SECURITY FORENSIC INVESTIGATIONS PRACTICE

- Navigant has a large team of computer forensic investigators across the US / Europe / Asia and is the preferred data security incident forensic investigations and response team for companies, cyber insurers, law firms, and brokers.
- Navigant's data security incident forensic investigations range from lost laptops, employee theft, ransomware (CryptoWall), and theft of trade secrets, to some of the most sophisticated hacking / malware incidents reported by the Wall Street Journal in 2012-2015.
- The firm has assisted clients for over a decade on hundreds of matters to investigate, analyze and help resolve the loss of business data and theft of trade secrets.

SOME INDUSTRIES SERVED:

Banks / Credit Union	Construction	E-Commerce Vendors	Energy	Engineers & Architects	Health Care Systems
Hospitality	Insurance Companies	Internet (Cloud Computing & Web Design Firms)	Law Firms	Managed Care Companies	Manufacturing
Municipalities / Government	Non-Profit Organizations	Parking Garages	Payroll Processing	Professional Services	Restaurants
Retail	Social Media	Software & Computer Hardware	Telecom	Transportation	Universities

INFORMATION SECURITY (PROACTIVE SOLUTIONS)	**POST-INCIDENT (REACTIVE SOLUTIONS)**
➢ **Enterprise-Wide Cyber Risk Assessment** ➢ **Penetration Testing / Anti-Phishing** ➢ **Business Interruption Calculation** ➢ **Vulnerability Scan Testing** ➢ **Tabletop Exercises** ➢ **Red Team Events** ➢ **Training**	➢ **Data Privacy Forensic Investigations** ➢ **Theft of Trade Secret Investigations & Litigation** ➢ **Business Interruption Calculation (IT / Damages)** ➢ **Malware / Systems Remediation** ➢ **Assisting With Regulatory Responses (FTC, Attorney Generals, DOJ)** ➢ **eDiscovery**

CONTACTS:

Darin Bielby
Director, Initiative Contact
215.832.4485
dbielby@navigant.com

Steven Visser
Managing Director
303.383.7305
svisser@navigant.com

Bill Hardin
Managing Director
312.583.4119
bill.hardin@navigant.com