Cyber Risk Report

A SurfWatch Labs Situational Awareness Report

December Attacks Highlight Need for Good Vulnerability Management

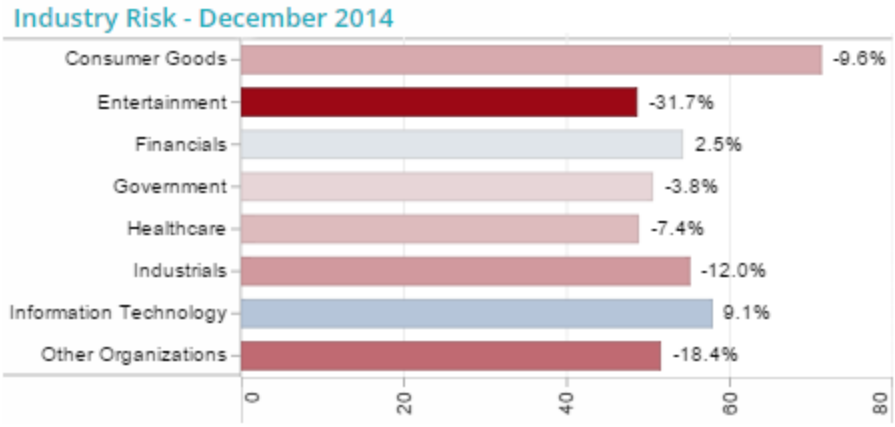
For the December 2014 Period

SURFWATCH
CYBER IN SIGHT

Cyber Risk Landscape – December 2014

The last month of 2014 saw an increase in risk among every sector but two: Financials and Information Technology.

Entertainment saw the largest jump (a 31.7% increase in risk score) compared to its six-month average, and Consumer Goods had the highest overall risk of any industry sector for the month. The cybercrime discussion in both sectors was dominated by the biggest story of the month, the breach at Sony Pictures Entertainment.



The overall industry risk scores for December 2014 and any change from the six-month average (red increased risk, blue decreased risk), based on SurfWatch Labs data.

December also saw widely reported denial-of-service attacks against Microsoft's Xbox Live network and Sony's PlayStation network. As usual, a handful of breaches and cyber-attacks received the majority of headlines, but there were many incidents that occurred throughout the month that did not gain widespread attention.

This report looks at four sectors in particular: Information Technology, Consumer Goods, Healthcare and Financials.

Key Trends and Conclusions at a Glance

- Disruptive attacks like denial-of-service attacks can cause significant damage to business operations and headaches for customers.
- In December criminals targeted several platforms used to comment and create content on websites.
- Cybercrime activity for the month was down in several sectors due to the holidays, highlighting the traditional organization of many cybercriminal groups.
- Retail data breaches continue unabated, but expect other types of attacks to accelerate as business transition to EMV cards, and force a shift in techniques used by cybercriminals.
- Stopping breaches entirely may not be possible, but advanced preparation will significantly decrease damage of a data breach.
- Supply chain cybercrime is an issue among all industry sectors, but Healthcare in particular – with regulations around protected health information and an assortment of partners from medical research institutions to third party billing – may be more susceptible than most.
- Ransomware and extortion will grow in 2015 as cybercriminals utilize the more direct route of payment for stolen information of extorting the victim.
- Massive attacks like the recent Sony Pictures breach often ripple through and have an impact on a variety of industry sectors; expect more large scale attacks like the one against JPMorgan Chase to occur this coming year.
- The focuses on large-scale breaches in the media can paint a misleading picture of cybercrime;, the little guys need to understand that they are both a target and often more susceptible to cyber-attacks – and take action.

SURFWATCH CYBER IN SIGHT

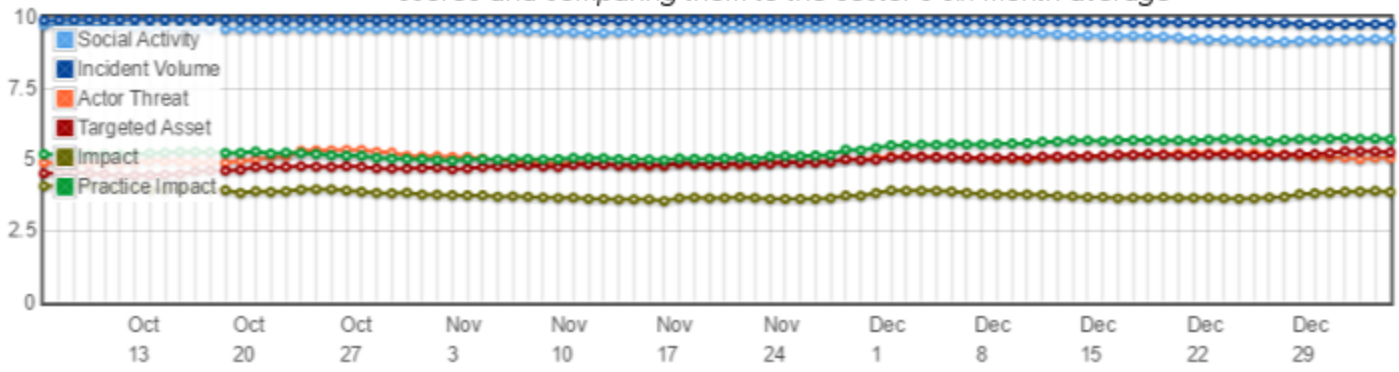
Information Technology Report Card

December 2014

B-

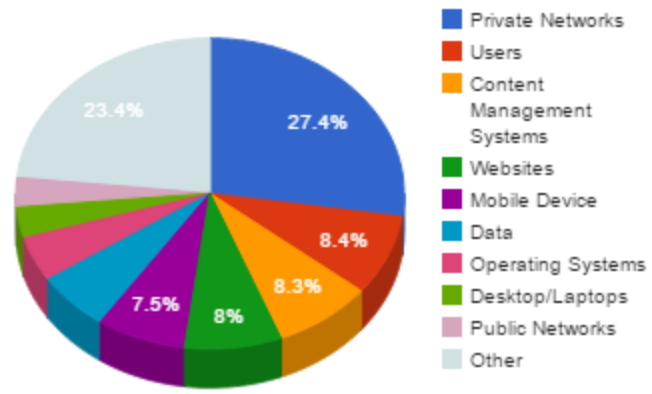
"Decrease in Risk"

SurfWatch Labs calculates an industry's grade by breaking down the month's CyberFacts into six weighted scores and comparing them to the sector's six-month average

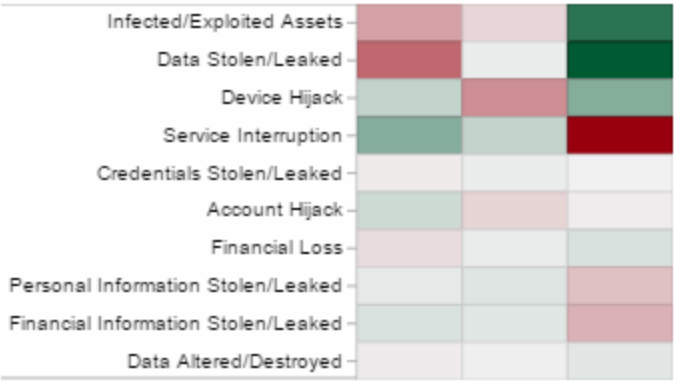


What's Everyone Talking About?

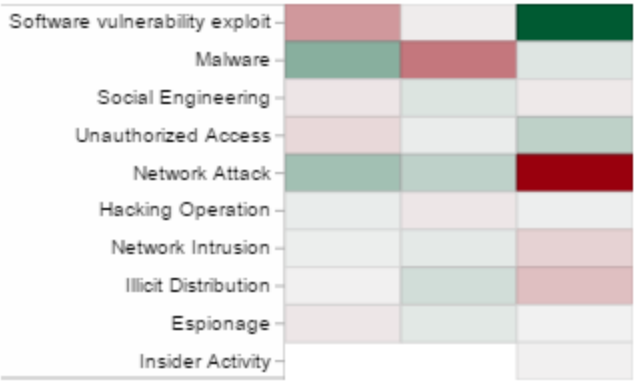
What are They After? (Target)



What Happened? (Effects) ___ Oct ----> Nov ----> Dec



How? (Practices) _____ Oct ------> Nov -----> Dec



The heatmaps show variation from the 90-day average (green lower %, red higer %) for the top 10 effect and practice.macro tags

SURFWATCH CYBER IN SIGHT

Information Technology Overview

Information Technology received a grade of "B-" for the month, indicating that the sector saw a decrease in cyber risk for the month when compared to the sector's six-month average. Service Interruption and Network Attack were the effects and practices that saw the biggest jump in December due to Lizard Squad's attacks on Sony's PlayStation network and Microsoft's Xbox Live network. Private Networks were by far the top trending target, accounting for more than a quarter (27.4%) of all the macro-level target tags in the sector. Usual industry targets like Microsoft, WordPress and Android generated the most discussion for the month.

Overall, despite Lizard Squad's disruptions, December had below average risk for the sector, likely due to the holiday season (criminals need a break too!), with Social Activity and Incident Volume both declining throughout December.

Activity and Events of Note

The Information Technology sector saw significant activity throughout the month. Several notable events occurred during the month including:

- ***Microsoft:*** Lizard Squad, a group of hackers, launched denial-of-service attacks on Microsoft's Xbox Live service. The hackers used a tool known as LizzardStresser to launch the attacks. Police arrested some alleged members of the group, but the group started marketing its tool as a criminal service soon after the disruption.
- ***WordPress -*** The SoakSoak malware infected an unknown number of websites running the WordPress blogging platform. The malware modifies a file in WordPress installation, then loads Javascript malware from the soaksoak.ru domain.
- ***Android:*** Researchers discovered that a pirated version of the popular Assassin's Creed mobile game was bundled with malware. The malware is designed to send multiple text messages, harvest texts from infected devices, and send stolen data to a remote C&C server.
- ***ICANN:*** The Internet Corporation for Assigned Names and Numbers (ICANN) admitted that in late November 2014 several members of their staff fell for a spearphishing campaign. The email campaign led to the loss of email credentials and the breach of several ICANN systems. The attacker also gained administrative access in ICANN's Centralized Zone Data System (CZDS).
- ***Plusnet*** : Customers of Plusnet, a UK Internet Service Provider (ISP), started receiving spam to email addresses given to the ISP for billing purposes. Customers complained to Plusnet, but the company denies that it was a victim of a breach. However, the UK's Information Commissioner's Office said it will review the claims and possibly investigate.
- ***Gigya***: The Syrian Electronic Army (SEA) used a DNS redirection attack on websites using the Gigya comment platform. Hackers from the group compromised Gigya's domain name record, redirecting users to sites with pictures of the groups logo or a photo claiming that the visitor's computer was compromised by the group.
- ***Facenama*****:** The popular Iranian social networking site, Facenama, suffered from a data breach. Hackers released details of 116,255 accounts. Data leaked included usernames, email addresses and their MD5 password. Members from Anonymous Iran have taken credit for the breach and leak.

Information Technology Conclusions, Trends and Predictions

Disruptive attacks like denial-of-service attacks can cause significant damage to business operations and lead to headaches for customers - Lizard Squad's attack on Microsoft highlights the effect disruptive attacks may have on a business. Additionally, it reinforces the cybercrime-as-a-service model, highlighting the widespread availability of criminal services.

In December, criminals targeted several platforms used to comment and create content on websites - The SEA targeted the Gigya comment platform and the unknown criminals targeted WordPress with the SoakSoak malware. Often criminals will targeted these third party platforms to gain unauthorized access to a website.

Activity for the month was down because of the holiday season - This highlights the surprisingly traditional organization of some cybercriminal groups. As with other businesses, employees often take time off during this time of year, sometimes slowing down business activity. Just like other organizations, organized cybercriminal groups may have been affected by employee vacations.

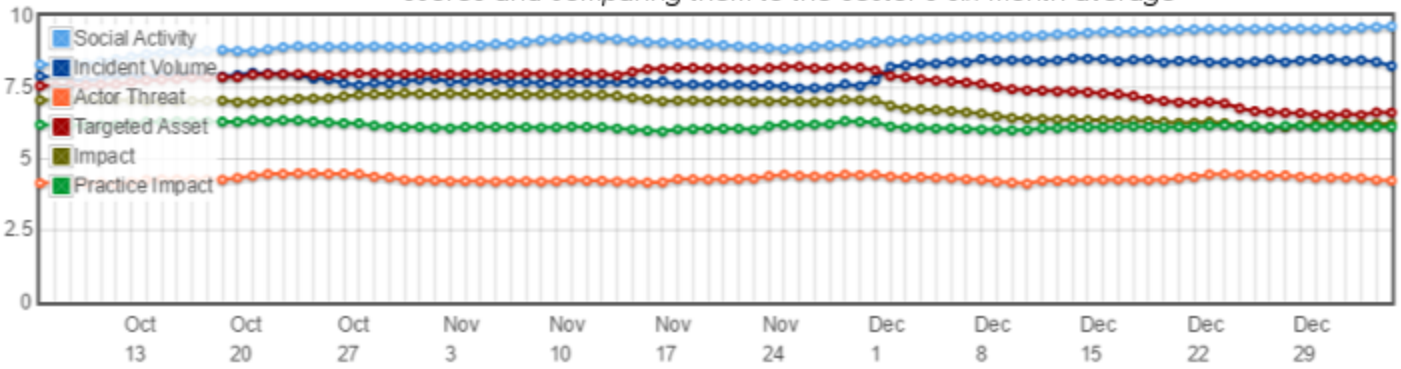
Consumer Goods Report Card

December 2014

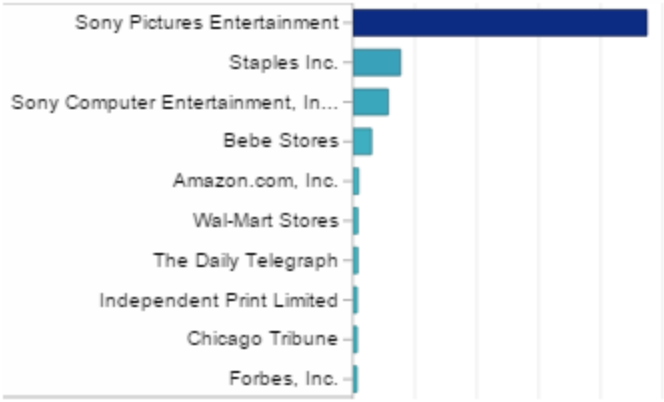
D-

"Significant Increase in Risk"

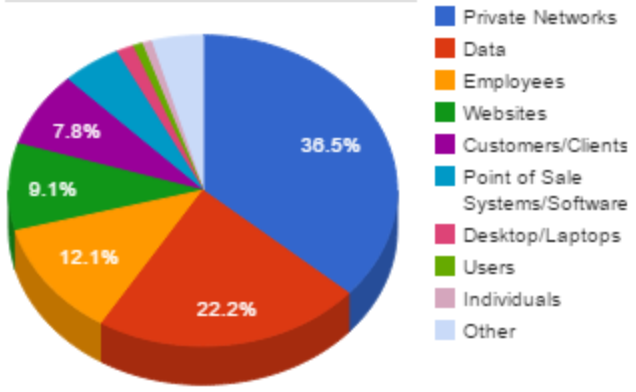
SurfWatch Labs calculates an industry's grade by breaking down the month's CyberFacts into six weighted scores and comparing them to the sector's six-month average



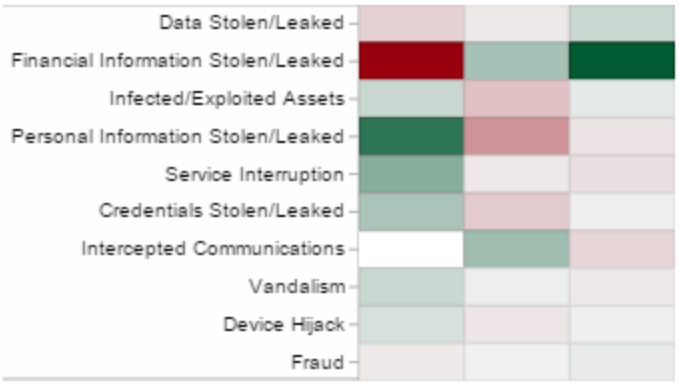
What's Everyone Talking About?



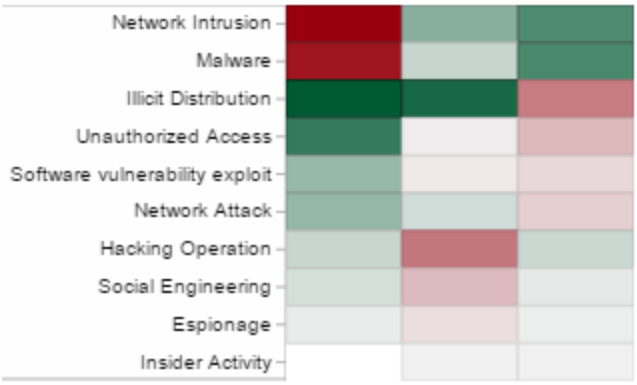
What are They After? (Target)



What Happened? (Effects) ___ Oct ----> Nov ----> Dec



How? (Practices) _____ Oct ------> Nov -----> Dec



The heatmaps show variation from the 90-day average (green lower %, red higer %) for the top 10 effect and practice.macro tags

SURFWATCH CYBER IN SIGHT

Consumer Goods Overview

Consumer Goods received a grade of "D-" for the month, indicating that the sector saw a significant increase in cyber risk for the month when compared to the sector's six-month average. Private networks (36.5%), data (22.2%) and employees (12.1%) were the top trending target macro tags for the month. Sony Pictures Entertainment received the bulk of attention for the month in terms of cybercrime discussion.

The Targeted Asset score for the sector went down, but other scores stayed stable or increased; there was much more Social Activity and Incident Volume, likely due to increased holiday shopping season attacks and media attention. The theft of financial information as an effect has notably decreased in recent months (much of the information stolen from Sony was not financial).

Activity and Events of Note

The Consumer Goods sector saw significant activity throughout the month. Several notable events occurred during the month including:

- ***Sony Pictures Entertainment:*** Fallout and revelations surrounding the Sony Pictures attack continued throughout December including the release of personal information on Sony employees, discussion around the data-destroying malware used in the attack, and the debate over state-sponsored hacktivism driven by the FBI's assertion North Korea was involved in the attack.
- ***Sony Computer Entertainment:*** Sony's PlayStation Network was brought down by Lizard Squad using a distributed denial-of-service attack during the Christmas holidays.
- ***Staples:*** Staples confirmed that 119 stores were impacted by a data breach from April to September 2014, compromising as many as 1.16 million customer payment cards.
- ***Bebe Stores:*** A data breach took place between November 8 and November 26, 2014, and affected those shopping in the retailer's stores located in the U.S., Puerto Rico, and the U.S. Virgin Islands, but not online or international.

Consumer Goods Conclusions, Trends and Predictions

Retail data breaches continue unabated - Size and frequency of retail data breaches vary from month to month, but the trend of payment cards being stolen through point-of-sale (POS) malware infections continues with seemingly little resistance.

Other types of attacks will take place and likely accelerate - As businesses transition to EMV (chip-and-PIN) cards for the October 2015 deadline, POS malware may lose much of its efficacy; this may prompt cyber attackers to transition to other techniques including ransomware and data-wiping malware, such as in the Sony Pictures attack.

Advanced preparation will significantly decrease damage of a data breach - It may not be possible to stop a major unexpected attack from a determined actor – such as the one affecting Sony Pictures – but the potential for damage can certainly be reduced. Poor password hygiene, lack of encryption, and unmanaged user privileges can increase the potential damage by eliminating barriers for intruders in the system. An early investment in preventative security measures will pay for itself when an attack occurs.

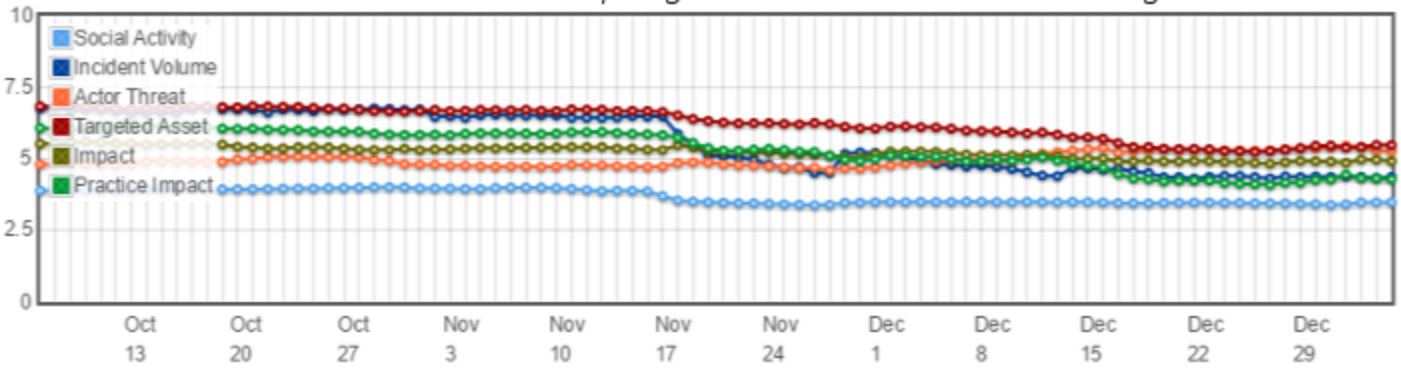
Healthcare Report Card

December 2014

C-

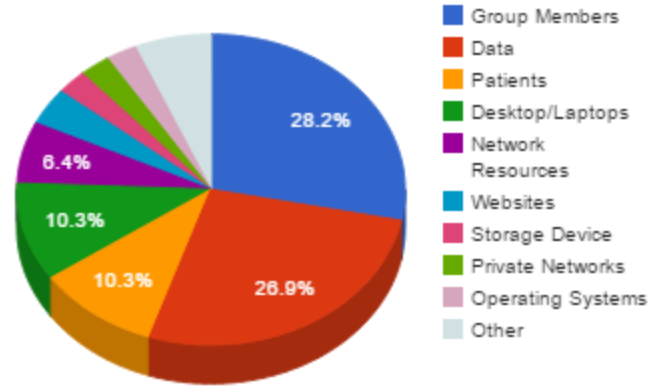
"Slight Increase in Risk"

SurfWatch Labs calculates an industry's grade by breaking down the month's CyberFacts into six weighted scores and comparing them to the sector's six-month average

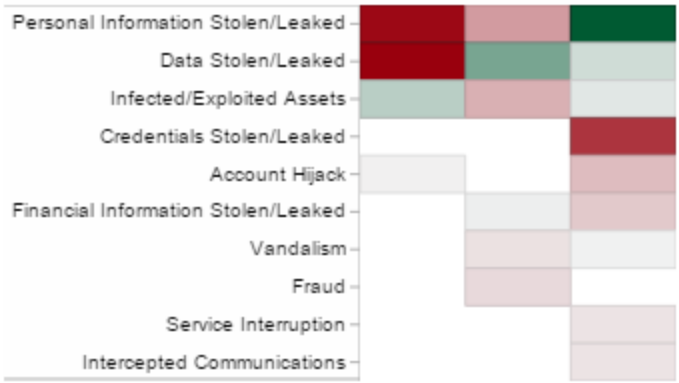


What's Everyone Talking About?

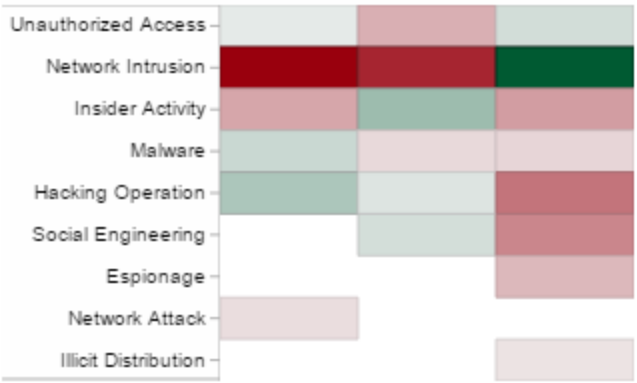
What are They After? (Target)



What Happened? (Effects) ___ Oct ----> Nov ----> Dec



How? (Practices) _____ Oct ------> Nov -----> Dec



The heatmaps show variation from the 90-day average (green lower %, red higer %) for the top 10 effect and practice.macro tags

SURFWATCH CYBER IN SIGHT

Healthcare Overview

Healthcare received a grade of "C-" for the month, indicating that the sector saw a slight increase in cyber risk for the month when compared to the sector's six-month average. Group members (28.2%), data (26.9%), patients (10.3%), and desktops/laptops (10.3%) were the top trending target macro tags for the month.

Looking at risk trends, the risk scores for Targeted Asset and Practice Impact continued their steady decline that began mid-November; however, the Actor Threat score saw a slight increase throughout the month.

Activity and Events of Note

The Healthcare sector saw significant activity throughout the month. Several notable events occurred during the month including:

- ***Highlands-Cashiers Hospital:*** The hospital notified more than 25,000 patients of a data breach caused by an error by IT vendor TruBridge. The information exposed included patients' names, addresses, birthdates, diagnoses and treatment information, health insurance information, and some Social Security numbers.
- ***WellCare Health Plans:*** 500 Medicare subscribers in New York were notified of a data compromise after a third-party vendor had a computer coding error causing denial letters to be sent to the wrong people. Social Security numbers were not affected.
- ***Lakewood Ranch Medical Center:*** A registered nurse at the medical center in Florida was arrested after it was discovered that she had been using patients' credit card information to make personal online purchases.
- ***Clay County Hospital:*** The hospital chain in Illinois reported a data breach after an unknown individual attempted to blackmail the hospital, demanding that a substantial payment be made to avoid patient data from being released. The information affected included names, Social Security numbers, and birthdates.
- ***The Kirkbride Center:*** A small number of paper documents were stolen from the medical center in Philadelphia. The documents contained information such as names, addresses, some Social Security numbers, birthdates, and some insurance and medical information. A total of 922 patients were notified.
- ***Reeve-Woods Eye Center:*** The eye center in California sent out a data breach notification letter after it was discovered that malware had been installed on two computers. The eye center has two facilities and one computer at each location had been affected.
- ***Mercy Medical Center Redding Oncology Clinic:*** A data compromise was discovered on December 13th, stemming from transcribed physician progress notes that were made publicly accessible by a third party website. The third party has since removed the link from their website.
- ***Corvallis Clinic:*** A laptop containing unencrypted patient data was stolen from an employee vehicle. It was not known how many patients were affected, but an investigation was being conducted by the Department of Health and Human Services.

Healthcare Conclusions, Trends and Predictions

Several healthcare breaches in December were caused by vendors and third parties - Supply chain cybercrime is an issue among all industry sectors, but healthcare in particular – with regulations around protected health information and an assortment of partners from medical research institutions to third party billing – may be more susceptible than most. While lost or stolen physical devices remains the most common breach story, there is a variety of potential attack vectors cybercriminals can use in the healthcare sector.

Ransomware and extortion will grow in 2015 - The recent extortion attempt on Clay County Hospital in Illinois highlights another potential problem: not only may cybercriminals steal valuable patient information, but they may go for the more direct route of getting paid and attempt to blackmail the victim. Most experts and law enforcement advise to never pay extortion attempts. Paying may lead to increased attacks due to being identified as a known source of income, and the criminals may still sell the stolen information to get another income stream from the same attack.

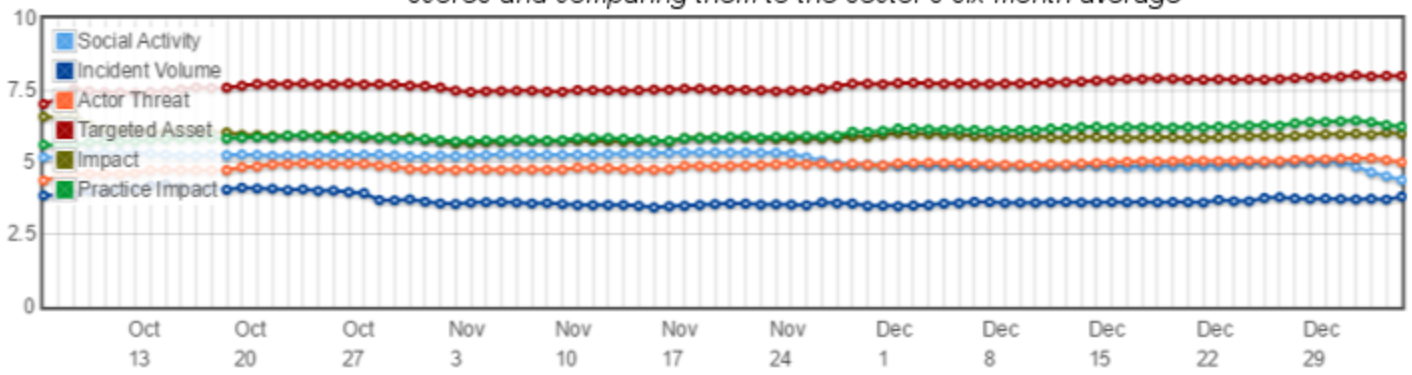
Financials Report Card

December 2014

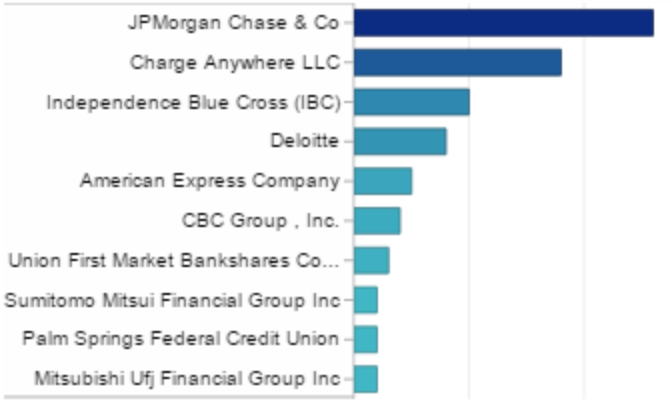
C+

"Slight Decrease in Risk"

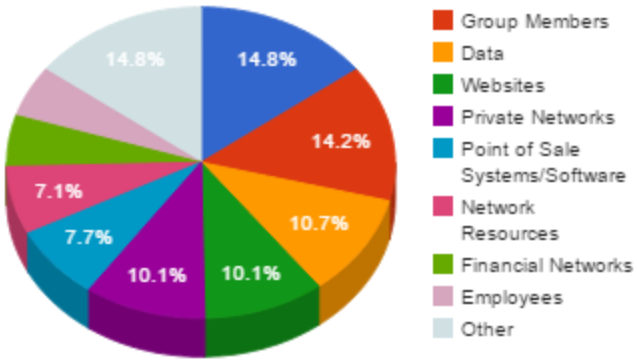
SurfWatch Labs calculates an industry's grade by breaking down the month's CyberFacts into six weighted scores and comparing them to the sector's six-month average



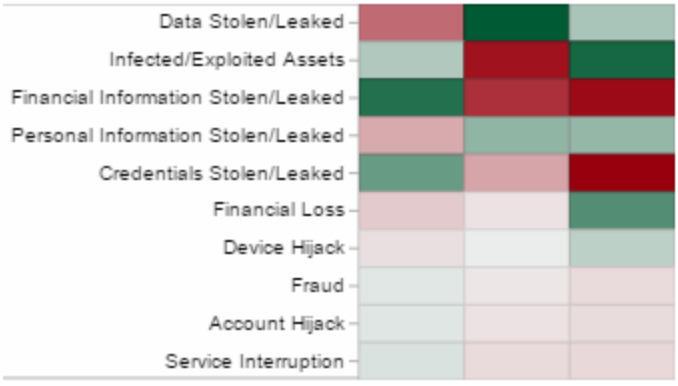
What's Everyone Talking About?



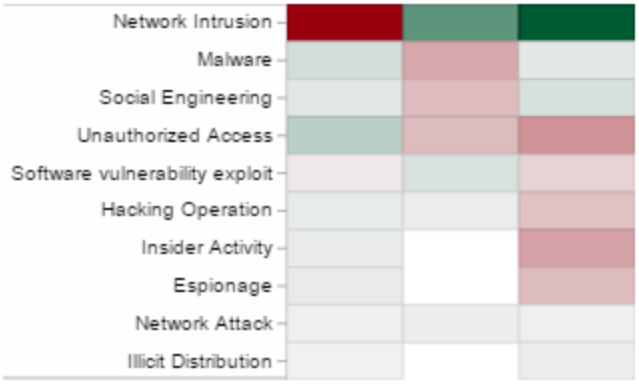
What are They After? (Target)



What Happened? (Effects) ___ Oct ----> Nov ----> Dec



How? (Practices) _____ Oct ------> Nov -----> Dec



The heatmaps show variation from the 90-day average (green lower %, red higer %) for the top 10 effect and practice.macro tags

SURFWATCH CYBER IN SIGHT

Financials Overview

Consumer Goods received a grade of "C+" for the month, indicating that the sector saw a slight decrease in cyber risk for the month when compared to the sector's six-month average. Most of the cyber risk held steady from October through December with Targeted Assets making the most significant increase toward December's end and Social Activity, which dipped in late November around Thanksgiving, dropping again over the December holidays. This is most likely due to the holiday's interfering with social reaction to events.

The most discussed industry targets for the month of December were JPMorgan and Chase, Charge Anywhere LLC, and Independence Blue Cross. When it came to specific macro-level targets, Customer/Clients (14.8%) and Group Members (14.2%) were the top trending categories followed by Data, Financial Networks, and Private Networks (all around 10%).

The top effects for December included Data Stolen/Leaked, Infected/Exploited Assets, and Financial Information Stolen/Leaked. For the Data Stolen and the Infected/Exploited Assets category there was a significant decrease in December and the Financial Information Stolen/Leaked showed a severe increase – most likely as a result of the revelations to the JPMorgan attack.

The top practices for December included Network Intrusion, Malware, and Social Engineering. All categories showed a decrease in December as some of the more mid-range practices increased during the month like Insider Activity.

Activity and Events of Note

The Financials sector saw significant activity throughout the month. Several notable events occurred during the month including:

- ***Independence Blue Cross:*** The company reported a data breach in late December after the discovery that an employee threw away four boxes of records related to customer data and member information. The data included the Social Security numbers of almost 9,000 people.
- ***JPMorgan Chase:*** The financial company remained steady in the news over December while investigations into its extensive data breach took place. The company reported the entry point for its attack in late December.
- ***Charge Anywhere LLC:*** In early December the company reported a data breach at the hands of malicious malware that made it past their virus protection and accessed thousands of credit cards from various merchants.
- ***Deloitte:*** The Sony Pictures hack didn't just affect Sony. The results of a gender pay study at Deloitte was released in the stolen documents showing a pay disparity in 2005 pay between the genders.
- ***Union First Market Bankshares Co:*** Union First Market Bank suffered a data breach at the hands of skimmers that affected more than 3,000 debit cards. The bank took immediate action to locate devices placed on ATM machines and halted cards affected by the breach.
- ***Palm Springs Federal Credit Union:*** A data breach occurred at Palm Spring Federal Credit Union after a National Credit Union Association Examiner reported a missing flash drive in his possession that contained personal data of bank employees and customers.

Financials Conclusions, Trends and Predictions

Massive attacks will ripple through all sectors - As seen with the recent Sony Pictures hack, the effects of one large-scale breach often reach into other sectors. These large attacks may become a trend due to the massive reach that some companies have, even if those companies may not expect to be attacked by hackers as they aren't directly connected to financial institutions or a wealth of specific personal data of value. The attacks will result in a larger scale intake of data (to sell or use for other purposes) as well as result in a wider news outcry.

The financial sector will continue to see its own brand of big attack - This year's JPMorgan attack resulted in the loss of data of millions. This happened despite the company spending millions on cybersecurity planning in hopes of protecting its data. One mistake can allow an attacker to slip through the cracks, and JPMorgan Chase won't the last. A year ago Target started the wave of huge breaches making news and it has continued to snowball this year, culminating in JPMorgan Chase and Sony Pictures level hacks.

Even the little guys need to take action - There is no doubt even small local credit unions need to protect their data from outside attacks. These massive attacks tend to dominate the news, but that doesn't mean that local banks can slack off on cybersecurity and training for their employees, as evident by the misplacement of a flashdrive in the Palm Springs Federal Credit Union data breach. Smaller organizations often make better targets for this very reason. No one is immune to cybercrime.

People, Process and Technology Countermeasures

When viewing the data elements from all sectors and their relative impact from malicious events for this period, SurfWatch Labs analysts determined that robust vulnerability management practices would have mitigated a large majority of attacks that industries suffered over the past month.

Adversaries desire two main capabilities when initiating an attack:

1. ***Privilege escalation -*** The act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. Attackers commonly take advantage of programming errors or design flaws to grant elevated access to the network and its associated data and applications.
2. ***Freedom of movement -*** The degree to which individuals or groups have – and perceive that they have – the ability to move from place to place within a given environment as well as into and out of that environment.

Lack of vulnerability management maturity within an organization directly enables adversaries to achieve a higher level of privilege escalation and freedom of movement, giving the attacker freedom to collect the items of value as well as doing so with a low risk of detection.

In order to reduce the potential for an attacker to achieve an increased privilege escalation and freedom of movement capability, organizations are strongly urged to review their vulnerability management practices in house as well as the method for how vulnerability management is accomplished.

SurfWatch Labs recommends reviewing for the following best practices when assessing a vulnerability management program.

What is Vulnerability Management?

Vulnerability management is the recurring practice of identifying, measuring, and mitigating vulnerabilities. This includes both patch management and operating system and application hardening.

- ***Patch management -*** A patch is an update to a software flaw that created a vulnerability in an operating system or application. Therefore patch management is the strategy and process used to determine what patches should be applied to which applications, and when.
- ***System hardening -*** System hardening is the process of securing a system by reducing its surface of vulnerability. This is generally accomplished by configuring the system to a state that only known and authorized functions are allowed to perform an action.

How Should Vulnerability Management be implemented?

Vulnerability management needs to be treated as a sustainment program that has a material effect on business resilience, especially since vulnerability management can easily be attributed as a key fault in an organization that is breached.

1. ***Needs to be repeatable:*** The vulnerability management program needs to be repeatable and measurable. Vulnerability “time to close” should be a core metric that the risk executive monitors on a routine basis and should rarely exceed thirty days for critical vulnerabilities.
2. ***Mitigation priority based on exposure:*** SurfWatch Labs data clearly reflects that attackers are focused on web-based attacks targeting the employee user base. Therefore when assessing systems for vulnerability management priority take an outside-in approach. First, if attackers are focused on web-based attacks with user focus, begin with the systems that the user utilizes on a daily basis such as user workstations. Second, focus on

the core business applications that the user base interacts with regularly such as employee intranet, time keeping, and consumer/customer and human resources applications. Lastly, focus on systems that have little general user population exposure and pivot towards applications that have a business unit focus, such as engineering, product or anything that has an intellectual property value.

3. ***Ensure you are using standard best practices in the vulnerability management program:***
    - Make it a daily duty of system owners.
    - Focus on the top five vulnerabilities of the day – every day – as a daily drumbeat and do not try to correct vulnerabilities in bulk.
    - Ensure you have a capability to correct third party application vulnerabilities (i.e. Flash, Adobe Reader, Java).
    - Use an industry standard benchmark for system hardening such as those published by the Center for Internet Security.
    - Utilize the common Scan, Test, Deploy, Re-Scan process when correcting vulnerabilities.

Vulnerability Management Tools:

There is a very robust vulnerability management vendor base both in free open source form and fee-based OEM vendors. Utilizing open source or fee-based OEM will usually be dictated by size of the organization. For small and medium-sized businesses, open source scanning tools may meet your needs; however, if enterprise scalability is a concern then OEM vendor tools are likely required. When selecting tools for vulnerability management, assess an organization's capability for the following tool types:

1. ***Enterprise vulnerability scanner -*** Scans for patches and system hardening vulnerabilities across the enterprise.
2. ***Application vulnerability scanner -*** Scans applications for flaws in coding. Tools are available for both web-based and non web-based applications.
3. ***Agent-based endpoint monitor -*** These tools typically offer a capability to push vulnerability fixes as well as give the ability to monitor device usage and performance. While scanners "find" vulnerabilities, endpoint agents generally allow the ability to "push" the fix.

Lastly, ensure that your supply chain and third party vendors deliver products or perform services with vulnerability management in mind, and ensure that contractual service-level agreements outline those requirements in detail. In many cases, products and services are delivered in a high-risk, vulnerable state because the organization did not have cyber security requirements outlined in the agreement. Your organization assumes that risk if contractual cybersecurity due diligence is not performed.