Hacked by a Nation-State.
Does Government Attribution Matter?
October 10, 2019
2:00 PM

Allison Bender
Wilson Sonsini Goodrich & Rosati
Direct: (202) 791-8028
ajbender@wsgr.com
WarGames, 1983
What is Cybersecurity?

“The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.” (Source: 2009 NIPP)
What is Cybersecurity?

“The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.” (Source: 2009 NIPP)
“National Security” means “those activities which are directly concerned with the nation's safety, as distinguished from the general welfare.”
Secure from What?

- **National security** – “I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter.”

- “**Cybersecurity threat**” means “an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term “cybersecurity threat” does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.”
“The loss of intellectual property and trade secrets through cyber espionage constitutes the greatest transfer of wealth in history.”

- NSA Director Alexander, July 2012
Cybersecurity Costs

Costs for businesses increased fivefold from 2013 to 2015 and are projected to reach $6 trillion by 2021. – Forbes estimate, 2017
Cost of a Data Breach Study 2019
by IBM Security and the Ponemon Institute

• Average consolidated total cost of a data breach is $3.92 million

• Average cost per lost or stolen record: $150

• Legal, financial and reputational harms are all considerations
Cost of Malicious Cyber Activity to the US Economy
The National Council of Economic Advisers, February 2018

• Estimated NYSE stock price reaction to public news of an adverse cyber event:
  • -0.8% in the first seven days, or
  • $338 - 498 million per adverse event
Intellectual Property Theft

• According to HBR, 80% of the value of the S&P as of 2015 was in intangible assets – intellectual property

• According to CNBC Global CFO Council Survey, Q1 2019 (US respondents only), more than 1 in 5 CFOs self-reported being a victim of Chinese intellectual property theft within the last year.

• Looking back 10 years in the same poll, that number grew to 1 in 3.
The potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits. The risk is growing that some adversaries will conduct cyber attacks—such as data deletion or localized and temporary disruptions of critical infrastructure—against the United States in a crisis short of war.
Cybercrime as a Percentage of GDP, 2015
Annual Cybercrime Revenue Estimates - 2018
$1.5T
Insider Threats

- Witting
- Unwitting
Ransomware and Doxing
Denial of Service Attacks
• Three Syrian nationals known to have defaced websites and media outlets in US, UK, France in support of Syrian government charged by DoJ in 2016

Social Media Hijacking

Breaking: Two Explosions in the White House and Barack Obama is injured
Social Engineering Customer Service

- Crackas With Attitude - 3 in UK; 2 in US
- Posted the message, "I own you," on the home TV of the US Homeland Security Secretary Jeh Johnson
- Left Johnson's wife a creepy voicemail message in which he asked: "Am I scaring you?"
- Accessed then-CIA chief John Brennan's AOL account and phone records
- Tweeted, e.g., "@CIA set your game up homies. We own everything. #freepalestine #CWA"
- Passed sensitive documents to WikiLeaks

At 18, Kane Gamble sentenced to two years in UK youth detention facility for actions as a 15 y/o.
Network Intrusions

PRE-ATT&CK

Priority Definition
- Planning, Direction
Target Selection
Information Gathering
- Technical, People, Organizational
Weakness Identification
- Technical, People, Organizational
Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

Enterprise ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control
Third Party Suppliers and Contractors

- In 2017, over 60% of reported attacks on public U.S. organizations were launched through the IT systems of third parties (suppliers or contractors).
  - This is an increase from <25% of attacks in 2010.
Two major breaches… of U.S. government databases holding personnel records and security-clearance files exposed sensitive information about at least 22.1 million people, including not only federal employees and contractors but their families and friends, U.S. officials said. Washington Post

Greg Touhill, less than a week after his resignation as the first government-wide chief information security officer (CISO), estimated that the cybersecurity breach at the Office of Personnel Management (OPM) could cost the government more than $1 billion in identity management solutions over the next decade. Symantec blog

The greatest damage caused by the massive Office of Personnel Management data breach wasn’t the loss of the documents themselves—it was the damage to the U.S. government’s reputation, current and former officials said Monday. “It’s a big deal in the sense that we need to renew the faith of the American public that we can protect that information,” said Charles Phalen, director of the National Background Investigations Bureau, the successor agency to OPM’s background check service the Obama administration stood up after the breach. Nextgov

“I don’t think there is recovery from what was lost,” said former CIA Director Michael Hayden, in a telephone interview with FedScoop. “It remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There’s no fixing it.” According to Hayden and other former CIA officers, the data breach has created a massive counterintelligence threat that could easily last 40 years — until the youngest members of the federal workforce enter retirement. FedScoop
Cyber-Enabled Influence Operations
Daily post count

POSTS PER DAY

- Vegas Shooting
- FISA Memo
- NFL Protests
- Syria Strikes
Tech Company Efforts

- Google banned a number of fake news sites from using Google Ads to monetize web traffic
- Facebook’s security team published the company’s first white paper on information operations, shedding light on how Facebook deals with state-backed actors peddling disinformation
- Red “disputed” tags on Facebook users’ feeds—an effort by the company to flag bogus content, but stopped after finding the system was ineffective, and that it often entrenched people’s beliefs rather than informing them
- Vigilance of social media companies during the recent French election allegedly did make a difference
- But, there are many examples of live or rapid viral content that still occur
Proposed Legislation, Regulation, and Industry Efforts

**US Honest Ads Act**
- Applies to any website, web application, search engine, social network or ad network that has 50 million or more unique U.S. visitors in a majority of months in a given year
- For campaigns that seek to spend more than $500 in total on political ads, tech and ad platforms would have to make new data about the ads available for public viewing - including copies of ads, information about the organizations that purchased them, audiences the ads might have targeted, and how much they cost.
- Would cover everything from promoted tweets and sponsored content to search and display advertising. And it includes ads on behalf of a candidate as well as those focused on legislative issues of national importance
- “Reasonable efforts” required to ensure that foreign governments and their agents are not purchasing political ads on their platforms

**US DISCLOSE Act**
- “Democracy Is Strengthened by Casting Light on Spending in Elections Act”
- Would require Super PACs and “dark money” political organizations to make donors public

**Germany - Netzwerkdurchsetzungsgesetz**
- “Network enforcement law”
- Aims to improve the enforcement of social media providers’ existing legal obligation to delete online content once they learn it violates German law
- Social media companies with over two million users must set up an effective procedure to process complaints regarding certain criminal offenses such as incitement to violence or defamation
- Must establish a system to delete all such “evidently unlawful” content within 24 hours, and less “evidently unlawful” content within seven days
- Neither the bill nor the Ministry of Justice provides a clear explanation as to what constitutes “evidently unlawful” content and what criteria social media platforms should use to make a determination. Additionally, it remains unclear how the law would be enforced.
- David Kaye, UN Special Rapporteur to the High Commissioner for Human Rights, criticized the responsibility the bill places “upon private companies to regulate the exercise of freedom of expression.”

**EU Code of Practice on Disinformation**
- Voluntary industry self-regulatory standards to fight disinformation
Robert Mueller charges Russian ‘troll farm’ with election interference

- Conspiracy and fraud charges against 13 Russian nationals and three organizations, accused of defrauding the United States as part of a campaign to influence the US election
- The defendants allegedly conducted what they called “information warfare against the United States,” with the stated goal of “spread[ing] distrust towards the candidates and the political system in general.”
- Media reports from a self-proclaimed Russian troll indicates House of Cards was training material on divisive US political issues
Cyber Command Russian Troll Farm Hack

• An unnamed government official disclosed to a WaPo reporter that on the day of the 2018 midterm election, Cyber Command shut down internet access at the Internet Research Agency (IRA), the Russian troll farm that ran an influence operation targeting Americans before the 2016 presidential elections, “to prevent the Russians from mounting a disinformation campaign that casts doubt on the results.”
NotPetya – A Case Study for the Impact of Government Action on the Private Sector

• NotPetya, June 2017, estimated to have inflicted over $1.2bn in damage
  – NotPetya was one of three major cyber-attacks, also including WannaCry and Petya, that used two exploits leaked from the US National Insurance Agency.
  • The first attack, Petya, was first discovered in March 2016, with WannaCry and NotPetya attacks taking place in May and June 2017 respectively.
  • NotPetya differed from the earlier WannaCry and Petya attacks in that it was not just ransomware. It was designed to masquerade as ransomware while committing as much damage as possible to systems within a network.

• Attribution
  – WannaCry was attributed to North Korea
  – Cybersecurity companies found that the NotPetya attack first struck in Ukraine.
  – In February 2018, first the UK, then the US, Canada and Australia publicly attributed NotPetya to Russia.
  – Russia denies involvement.
In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.

The attack, dubbed “NotPetya,” quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin’s ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia’s involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.
Mondelez v. Zurich

- $100 million lawsuit filed in October 2018 by Mondelez, the maker of Oreos and Cadbury chocolate, against its insurer, Zurich Insurance Group, regarding a claim the company made for damages incurred from the NotPetya attack
  - Mondelez claimed
    - $100 million on its insurance policy permanent damage to 1,700 of its servers and 24,000 laptops, inflicted by NotPetya, plus the theft of thousands of user credentials, unfulfilled customer orders and other losses
    - Argued damage and losses fell under the provision of its insurance policy that covered “physical loss or damage to electronic data, programs, or software” caused by “the malicious introduction of a machine code or instruction”
  - Zurich declined coverage arguing NotPetya, the virus introduced to the Mondelez servers, was orchestrated by the Russian military – and damages are therefore not covered by the policy Mondelez purchased, due to an exclusion under an act of war exclusion for “hostile or warlike action in time of peace or war” by a “government or sovereign power.”
Data Breach Prevention

Despite concerns about “zero-day” vulnerabilities or the inability to combat complex attacks, the vast majority of breach incidents fall into four categories:

- Human error or negligence
- Compromised credentials
- Failure to patch known security flaws
- Insider threats

While no organization can claim 100% security, these threats are knowable, manageable, and addressable. In April 2018, Dave Hogue, Technical Director of the NSA’s Cybersecurity Threat Operations Center publicly disclosed:

- In the previous 24 months, the NSA had not responded to a single zero-day attack on its systems
- 90% of security incidents at NSA in the prior year were caused by human error; 93% could have been prevented through use of best practices
Opportunities for Data Breach Cost Savings

**Effective Governance**

- **$1 million** - average savings for incident response efforts concluded within 30 days of breach discovery ($3.09M v. $4.25M average total)
- **$340,000** - average savings for organizations with an incident response plan
- **$14 per record** - average savings for organizations with an incident response team (in-house, third party, or combination)
- **$13 per record** - average savings for organizations with a business continuity plan and related management controls in place

**Technology Investments**

- **$1.5 million** - average savings for organizations that extensively deployed automated security technologies ($2.88M v. $4.43M average total)
- **$8 per record** - average savings for organizations using AI for cybersecurity

Source: Cost of a Data Breach Study IBM Security and the Ponemon Institute, 2018
Involving the Federal Government

• Report incidents that:
  – result in a significant loss of data, system availability, or control of systems;
  – impact a large number of victims;
  – indicate unauthorized access to, or malicious software present on, critical information technology systems;
  – affect critical infrastructure or core government functions; or
  – impact national security, economic security, or public health and safety.

• But be prepared - How will a government investigation impact your:
  – Insurance notice of claim;
  – Internal and external communications strategy and timing;
  – Regulatory filings;
  – Etc.
Questions?

Thank you!

Allison Bender
ajbender@wsgr.com