NORTON ROSE FULBRIGHT

Cyber Security: Real Examples, Mitigation, and Additional Threats

David J. Kessler
Global Head of Information Governance and E-Discovery; U.S. Head of Privacy
September 23, 2021


Georgia Secretary of State Office 2015 breach
SC Department of Revenue 201 Data Breach – "South Carolina Breach Compromise of Records"
– GovTech
NOAA Reveals Four Websites Compromised
– GovInfoSecurity
New York City Law Department Hit by Cyberattack
Email systems breached at the Treasury and Commerce Departments - "Russian Hackers Broke Into Federal Agencies, Official Suspect"
– York Times
Government payment site leaks million customer records"
– adget
Email systems breached at the Treasury and Commerce Departments - "Russian Hackers Broke Into Federal Agencies,
Probe Targets Archives; Handling of Data on 70 Million Vets
– Wired
alifornia Doesn't Know What It Did With 800,000 Child Support Records"
– Business Insider
Flordia Sheriff's Office Hacked
– Data Breach Today
Security
Buildings in
– U.S. Government Accountability Office
LA County data leak: 3.2 million files containing sensitive details of callers to crisis and abuse hotline exposed
Veterans Affairs Data Privacy Breach: Twenty-Six Million People Deserve Assurance of Future Security
nt (OPM) data breach: "Government Data Breach Affects Millions of Americans"
– Lifelock
Probe Targets Archives; Handling of Data on 70 Millio Vets
– Wired
Data exposed
– Reuters
Security breach discovered at the Oregon Employment Department; investigation into scope, source continues
– OregonLive
Leads to Breach at fornia State Controller
bs on Security
Washington State system hacked, data of thousands at risk
– Reuters

“There are only two types of companies: those that have been hacked, and those that will be.”

- Robert Mueller, FBI Director, 2012.

"[There are only two types of companies:] companies that have been hacked and will be hacked again.“

- Robert Mueller, FBI Director, 2012

Agenda

- Examples of Government Cyber Incidents
  - Federal Government
  - Ohio Incidents
- Lessons Learned
- What is on the Horizon

Question 1:

Has your current or past organization been the victim of a threat actor gaining access to its IT environment and causing a cyber incident?

* Yes
* No
* Don’t Know

Question 2:

If you answered “Yes” to Question 1, did the organization provide written notice to individuals, regulators or both?

* Yes, provided notice to both
* Yes, only to regulators
* Yes, only to individuals
* No
* Don’t know

Types of Cyber Incidents – Third Party/External

- Denial of Service Attacks
- Business Email Compromise Attacks
- Supply Chain Attacks
- Ransomware Attacks
- Exfiltration
  - Data Mining / Identity Theft
  - Corporate Espionage
  - Leverage for Ransom

Question 3:

Which Cyber Incident poses the greatest risk to consumers and employees?

* Denial of Service
* Business Email Compromise
* Supply Chain Attacks
* Ransomware
* Exfiltration for Espionage
* Exfiltration for Data Mining
* Exfiltration for Leverage

Federal Government Agencies

U.S. Office of Personnel Management (OPM) (2015)

- Chinese state-sponsored hackers exfiltrated approximately 25 million records, including names, dates and places of birth, addresses and Social Security numbers related to government employees, other people who had undergone background checks, and their friends and family.
- Two separate, but linked, attacks:
  - First attack: date unknown – discovered March 20, 2014
  - Second attack: May 7, 2014 (attackers posed as subcontractors) – discovered April 15, 2015
- Director and CIO of OPM resigned
- Federal employee unions filed a lawsuit against OPM in which the DC Court of Appeals found that "OPM effectively left the door to its records unlocked by repeatedly failing to take basic, known, and available steps to secure the trove of sensitive information on its hands. *In Re: Office of Personnel Management Data Security Breach Litigation*, No. 1:15-mc-01394 at 30 (June 21, 2019).
- The case is ongoing.

PACER (2014)

- Hackers attacked the Public Access to Court Electronic Records (PACER) system.
- The entire system was affected for approximately four hours and disabled the filing of pleadings and orders.
- The hackers were able to access federal court filings, including those that had been filed under seal and others that contained sensitive personal information.

SolarWinds (2020)

- Russian intelligence agencies compromised SolarWinds Orion (a monitoring software) to deploy malware on systems of 18,000 SolarWinds customers, including several US government agencies:
  - Department of the Treasury
  - Department of Commerce (incl. National Telecommunications and Information Administration)
  - Department of State
  - Department of Labor
  - Department of Defense
  - Department of Homeland Security
  - Department of Energy
- The full extent of the incident is still pending investigation.

OHIO
City/State Government Agencies

Examples

- Cleveland Hopkins International Airport:
  - Malware detected on computers that led to interference with baggage claim operations and flight and baggage claim screens were down for almost a full week.
  - Remediation costs reached almost $2 million.
  - It does not appear that any personal information was involved.
- Toledo Public Schools
  - Toledo Public Schools fell victim to a ransomware attack that led to the school board taking its systems offline and cease virtual education on the first day of online learning for the school year.
  - Data included names, dates of birth, addresses, Social Security numbers, and information related to one's employment or academic history.
  - Many victims have alleged identity fraud as a result of the incident; however to date there has been no litigation or civil enforcement against the district.
- City of Geneva, Ohio
  - Town of 6,200 experienced a ransomware attack in early July 2021.
  - Some citizens Social Security numbers and credit card numbers may have been exposed, but the investigation is ongoing.

Ohio Department of Job and Family Services (2021)

- Two separate incidents in 2021
- Incident 1: Data exposed due to glitch in computer system (January 2021)
  - Affected information of 146 Ohioans – data included names, addresses, phone numbers, driver's license numbers, and Social Security numbers.
  - Affected individuals were applicants for Pandemic Unemployment Assistance benefits.
  - According to the Department, no personal information was misused.
  - To date, there has been no civil enforcement action or litigation as a result of the incident.
- Incident 2: Fake unemployment site (April 2021)
  - Unemployment site housed by Russian server impersonated Ohio Dept. of Job and Family Services website
  - Undetermined number of Ohioans received text messages directing them to the site to enter tax and banking information to receive "unemployment benefits"
  - Total number of affected individuals is unclear

Attacks on Law Enforcement

- Westlake Police Dept., Cayahuga County (February 2021)
  - Threat actors attacked the Westlake Police Station and deleted records of police dash-cam recordings. The ransomware never demanded a payment and instead froze police computers deleting evidence.
- Butler County Sheriff's Office (December 2020)
  - Malware disabled the Computer Aided Dispatch (CAD) system for approximately 10 days, causing dispatchers and the crews they were sending to emergencies to resort to maps and pens and papers. The attack caused almost $180,000 in costs for equipment, repairs and overtime (the county's insurance paid nearly $70,000).
- Ross County Sheriff's Office (October 2020)
  - Malware attack spread through documents in email to the entire Sheriff's office network, exposed payment information, social security numbers, police reports, 911 calls and more.

Mitigation

Basic Mitigation Steps

- Easy to Say – Hard to Implement
- Universal Multi Factor Authentication
  - Remote Connection and Financial Account Changes
- Do Not Ignore the Human Element
- Operational and Test DR/BC
- Reasonable Information Governance Program
  - Privacy and Cyber Forward
  - Dispose of ROT (Residual, Obsolete and Trivial) Data

Question 4:

My organizations record retention policy and schedule are best described as?

- **A well understood and followed set of guidelines that enable employees to dispose of data;**
- **Guidelines that we are trained on but are never addressed again;**
- **A set of papers and materials that sit on the shelf;**
- **I do not know if we have a policy and a schedule.**

Cyber Defense Strategies

- Ohio Cyber Range
  - The Ohio Cyber Range, opened in May 2018, is a secure virtual environment used for cybersecurity training and technology development. It is accessible for competitions, training and as a testing environment for schools, governments and businesses.
  - Range sites are located at the University of Cincinnati and the University of Akron.
- Ohio National Guard Cyber Force
  - Supports and defends state agencies and critical infrastructure in Ohio. Ohio National Guard members leverage their military-specific training with cyber expertise they bring from their civilian jobs to assist in emergency response.
- Ohio Cyber Reserve (OhCR) created October 2019
  - On October 25, 2019, Ohio Gov. Mike DeWine signed legislation forming the Ohio Cyber Reserve, a volunteer cyber force under the supervision of the Adjutant General's Department to assist local governments affected by cyberattacks. It is composed of trained, vetted Ohio civilians.
  - OhCR teams are based in five regions throughout the state and its members, provided with training, equipment and credentials, work out of Ohio National Guard readiness centers.

Additional Threats

Question 5:

What is your biggest cyber fear over the next 3-5 years?

- **Financial fraud enables major theft**
- **Ransomware shuts down my organization and we cannot recover**
- **Personal data is stolen and published on the Dark Web**
- **Data destruction or data corruption**
- **Other**

Current trends

- Nation-state intrusions: growing frequency and severity, often with the aim of carrying out monitoring/ profile building / IP theft / financial gain. Key threat Actor Groups include APT 19 (China) – espionage/monitoring/tracking; APT 39 (Iran) – monitoring/tracking/surveillance.
- Credential stuffing and password spraying
- Ransomware and disruptive malware attacks
  - Ransomware combined with exfiltration; strains and modules evolving
  - Growing in prevalence, with the malware attacks often aimed at causing operational disruption in key industry sectors – more targeted “big game hunting” than previously
  - Malware-as-a-service
- Business email compromises: continue at alarming rates
- Public Scrutiny: The public (and, therefore, State legislatures and Congress) are taking a much more active look.
- Firmware and IoT: Because more things are web-enabled, cyber incidents can have more direct impact on the physical world

NORTON ROSE FULBRIGHT

Law around the world

nortonrosefulbright.com