Best Practices in Cyber Incident Response

April 16, 2024

Dismas Locaria
Partner | +1 202.344.8013 | dlocaria@Venable.com

John Banghart
Senior Director for Cybersecurity Services | +1 202.344.4803 | jfbanghart@Venable.com

Sabeen Malik
Vice President, Global Government Affairs and Public Policy | 202-779-2123 | sabeen_malik@rapid7.com

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Diz Locaria assists government contractors and grant recipients in all aspects of doing business with the federal government. Diz has extensive knowledge of government contract and grant regulations, enabling him to help organizations qualify to become federal contractors or grantees. He represents clients in compliance with various federal procurement and grant requirements, including ethics and integrity; mandatory disclosures; False Claims Act; responsibility matters, such as suspension and debarment; small business matters; and General Services Administration (GSA) Federal Supply Schedule contracting. Diz also represents and counsels clients regarding the Homeland Security Act, including obtaining and maintaining SAFETY Act protections.

John Banghart leverages his significant federal government and private sector experience in cybersecurity to navigate issues related to risk management, government policy, standards and regulatory compliance, and incident management. He has successfully led efforts to address significant and high-profile cybersecurity issues within major government programs and institutions while facing complex legal, technical, and political circumstances.

Sabeen Malik is the Vice President of Global Government Affairs and Public Policy at Rapid7. She has spent her education and career pursuits becoming a thought leader on digital economy and tech policy issues, law and economic development, innovation economies, and next-generation emerging technology and economic trends. Sabeen has worked in the private and public sector, including at Thumbtack, Google, and the United States Department of State where she served as a senior tech advisor to the Under Secretary of State for Economic Growth, Energy, and the Environment. Along with a passion for global technology trends in business and economic issues, she also is an expert on bridging differences with the public and private sector to create international partnerships that solve global problems. Sabeen serves on several boards and is a Truman National Security Fellow, Aspen Socrates Fellow, Atlantic Council Non Resident Fellow, and Stimson Loomis Council member. She has spoken at the World Bank, the UN, and the White House.

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Common Causes of Cybersecurity Incidents

A cyberattack is any form of malicious activity attempting to gain unauthorized access to IT systems and data. Below are the some of the most common types of attacks:

1. Malware
   - Any intrusive software to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, viruses, spyware, and **ransomware**
2. Phishing
   - The use of deceptive emails that appear to come from a reputable source with the goal of stealing sensitive data such as financial information
3. Denial of Service (DoS) and Distributed Denial of Service (DDoS)
   - A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth, causing the system to become unavailable
4. Data Breach
   - Loss of confidentiality, integrity, or availability of sensitive information, such as personal data or intellectual property

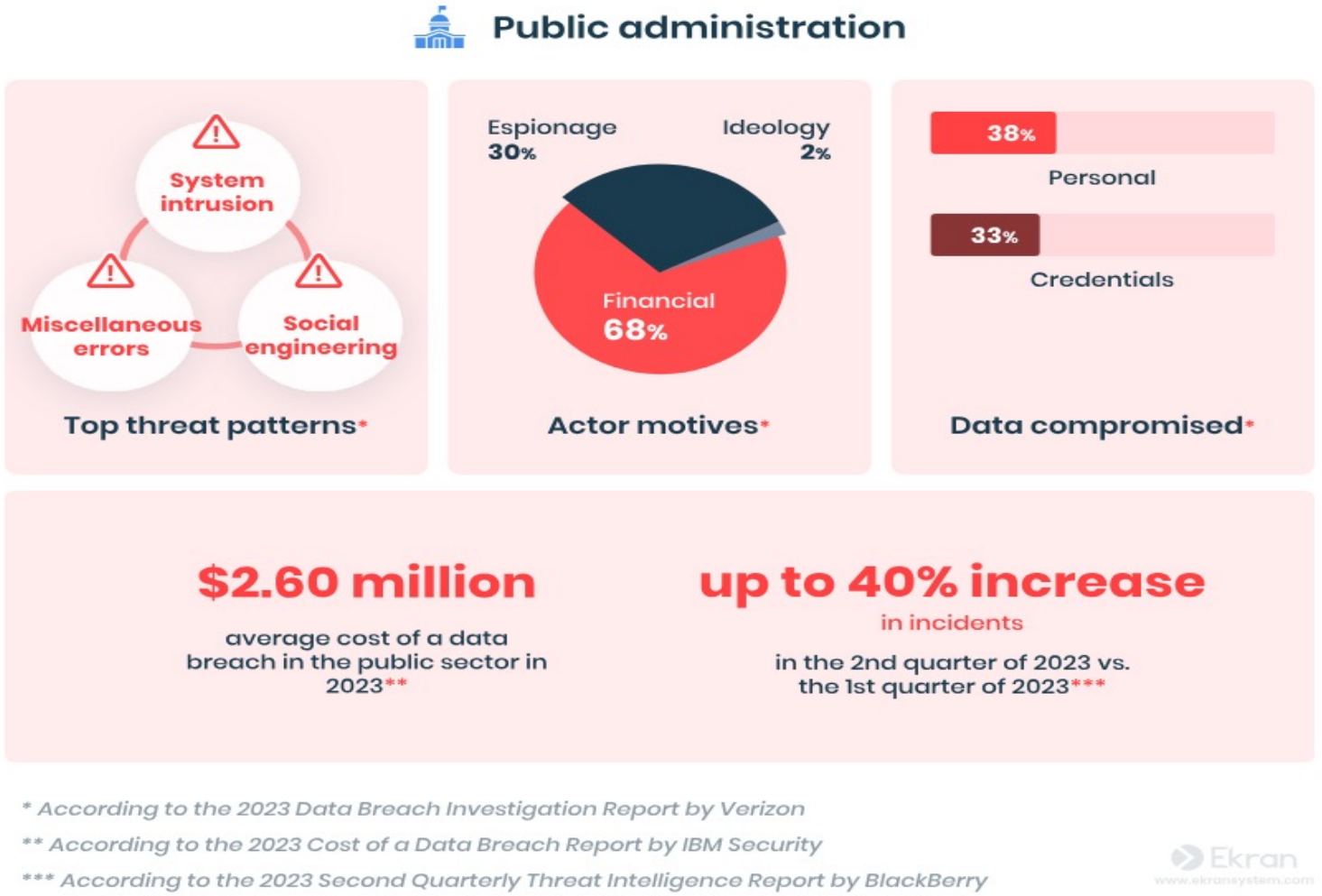
Attackers will frequently use more than method to get what they want.

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Cyber Threat Landscape

Government agencies and contractors are frequent targets for nation-state (e.g. Russia, China) sponsored attackers looking for information that can be used for espionage, economic advantage, or mission-disruption.



VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

The Role of Law in Cyber Incidents

- **Protection**. As cybersecurity incidents lead to extraordinary economic and national security consequences, the role of the law in cybersecurity is to help establish a framework for protecting individuals, organizations, and governments from cyber threats.

- **Transparency**. Many cybersecurity laws are aimed at encouraging information sharing and cyber incident reporting to government, industry sectors, or the public. This transparency can help head off threats and focus defense resources.

- **Deterrence**. Cybersecurity laws and penalties have been developed to deter cybercrime, as well as lax security for personal information and critical systems.

VENABLE LLP

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

Factors That Determine Legal Consequences

Not all cyber-attacks raise the same legal implications. Specific circumstances dictate which laws and regulations come into play. Below are non-exclusive factors that influence the legal consequences of cyberattacks:

- The entity's industry/sector
- Categories of data impacted (e.g., Protected Health Information)
- Affected individuals' location of residency (including end users and employees)
- Contractual obligations that incorporate laws by reference
- Reasonableness of entity's security risk management program and due diligence
- Conduct/involvement of entity's employees, management, agents, etc.; and
- Severity of impact of the incident

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Legal Implications of Cybersecurity Incidents

- **Cyber Incident Reporting and Data Breach Notification:**
  - Mandatory Reporting:
    - *Breach Notification* - Entities are often required to report data breaches to affected individuals, regulatory authorities, third parties, and in some cases the media.
    - *Incident reporting* – Increasingly, entities are required to report cyber incidents, even if personal information is not affected. Some laws may require ransomware payment reporting.

- **Regulatory Penalties:**
  - Timely Disclosure: Failure to promptly disclose breaches or incidents can result in significant penalties and fines.
  - Reasonable Security: Different sectors and jurisdictions require organizations to have reasonable security for sensitive data (i.e., personal information) and systems (i.e., critical infrastructure).

- **Additional Liability:**
  - Large-scale breaches can lead to class action lawsuits where affected individuals collectively sue for damages.
  - Organizations and executives can be held liable for inadequate cybersecurity measures. See, for example, FTC's actions regarding Drizly.

VENABLE LLP

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

Legal Requirements for Cybersecurity Incidents

Generally, these are requirements that covered entities must comply with under most legal frameworks:

1. **Prevention**: Establish a security risk management program to protect against threats.
2. **Incident Response Plan**: Have a written plan with processes and roles for incident response.
3. **Respond to the Incident**: Detect, contain, and mitigate the incident.
4. **Incident Reporting**: Report breaches and incidents within designated timeframes and formats.

Here are some of the common legal frameworks that require these requirements:

- Health Insurance Portability and Accountability Act (HIPAA)
- New York Department of Financial Services Cybersecurity Regulation (NYDFS)
- Payment Card Industry Data Security Scorecard (PCI DSS)
- General Data Protection Regulation (GDPR)
- NIS 2 Directive

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Incident Response Stages

- Verification of Breach:
  - Identify affected systems and cause of incident
- Containment and Mitigation:
  - Take reasonable actions to stop attacker and mitigate the attack vector
- Investigation and Analysis:
  - Obtain organization's incident response plan and convene incident response team
  - Initiate forensic analysis on the cause of the incident
  - Engage third parties to assist, which may include Outside Counsel for privilege purposes, Forensics Vendors, Communications Team, etc.
- Notification:
  - Develop notification plan if notification is required
  - Identify parties to be notified
  - Identify notification timelines
- Post-Notification and Response Review:
  - Review incident response processes to identify lessons learned or necessary changes to incident response policies/procedures
  - Continue apprising notified parties of further information and corrective measures, as necessary and/or appropriate

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Real-Life Case Studies

International humanitarian organization (2021)

- **Description of Incident**: Attackers accessed a database that contained names, addresses, and contact information for 515,000 people separated from their families by war and natural disasters.
- **Impact of strong incident response plan**: The organization's response was swift, transparent, and comprehensive. With a coordinated team, they quickly posted a lengthy FAQ on their website that described the hack, immediately took the compromised servers offline, quickly deployed enhanced security measures, conducted external penetration tests, and reached out to those affected.

Money transfer service (2021)

- **Description of Incident**: An employee who had regular access to customer account data while employed at the company accessed those reports without permission after their employment ended. The employee downloaded data of 8.2 million customers. Entity discovered the breach in Dec. 2021, but failed to disclose the information to SEC until Apr. 2022.
- **Impact of weaker incident response plan**: Many customers had unauthorized charges made against their accounts and, in a class lawsuit, pointed out that the entity's delay in notifying users of the breach caused additional harm to customers that "they otherwise could have avoided had a timely disclosure been made."

General Best Practices

- Make use of risk based international cybersecurity standards and frameworks
  - NIST CSF, ISO/IEC 27000 series
- Acquire and maintain cyber insurance
- Conduct exercises
  - Technical exercises for IT team with forensic partners
  - Decision-making / leadership exercises (seminars, workshops, etc)
  - Tabletop exercises (Scenario and Module Questions)
- Engage with third parties to augment existing capabilities and fill gaps
  - Identity the appropriate members assisting with organizational responses (e.g., legal, security, communications)
  - Consider bringing third parties in through counsel to secure application of attorney-client privileges
- Develop a regulatory notification chart to keep track of the different incident reporting obligations

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Coordination Stakeholder Mapping and Exercises for Incidents

- **Identify** stakeholders
- **Define** a process
  - Is there overlap between regulations if you are affected by more than one? If so, use the most stringent as a baseline for policy creation
  - Document the requirements along with the process and procedures to meet those requirements in the worst-case scenario, including templates for notifications to government entities
  - Have a clear communication strategy that has been passed through legal and PR
- **Define** best practices and principles for your company's view on transparency and disclosure – should not be case by case or made during the response
  - before,
  - during, and
  - after an incident
- **Coordinate** public-facing artefacts that may be submitted to the federal government partners

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Coordination for Reporting on Incidents

- **Principles – PPD 41/EO 14028**
  - Shared Responsibility
  - Respecting Affected Entities
  - Unity of Governmental Effort
  - Enabling Restoration and Recovery
- **Government Coordination**
  - Incidents found by the company:
    - Report Cyber Incidents to the Federal Government. Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies and their sector-specific agency.
    - The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.
  - Incidents found by the government:
- CIRCIA Proposed Rule Making issued on 4/4/2024 and 60-day comment period

VENABLE LLP

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

Thank you!

Dismas Locaria
Partner | +1 202.344.8013 | dlocaria@Venable.com

John Banghart
Senior Director for Cybersecurity Services | +1 202.344.4803 | jfbanghart@Venable.com

Sabeen Malik
Vice President, Global Government Affairs and Public Policy | 202-779-2123 | sabeen_malik@rapid7.com

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION