Debevoise & Plimpton

Lawyers Alliance FOR NEW YORK
Connecting Lawyers, Nonprofits, and Communities

Cybersecurity for Not-for-Profit Organizations: Tips on Preparing for, and Responding to, Cyber Attacks

Jennifer Cowan
Luke Dembosky
Liz Guggenheimer
Suchita Brundage
Mengyi Xu

March 2, 2022

Our Discussion Today

Evolving Threat Landscape

Key Non-Technical and Technical Preparations


Evolving Threat Landscape

Phishing

- Email phishing remains the most common method by which cybercriminals first gain unauthorized access into a target's environment, which can then lead to ransomware incidents, business email compromise scams and other destructive cyber attacks.
- With the ongoing pandemic and remote work arrangements, cybercriminals are increasingly leveraging well-known brands—like Microsoft Teams, Zoom and Skype to launch social-engineering schemes.
- According to CISCO's 2021 Cybersecurity Threat Trend report, about 90% of data breaches occur due to phishing.

Source: https://www.debevoisedatablog.com/2020/06/25/phishing-testing-for-employees-what-to-do-with-those-who-fail/

Credential Stuffing

- As more of our activities move online, the number of passwords we require increases. The tendency to reuse passwords increases the risk of credential stuffing attacks.
- In a credential stuffing attack, a threat actor takes stolen credentials purchased from a data breach of one account (or through their own phishing and hacking activities) and tries to use them to access a different account, typically many other accounts, through an automated, brute force attack.
- The result is that all of the accounts that use the same login credentials are vulnerable if any one of them is compromised
- Like phishing, credential stuffing is often not an attack by itself, but a means to gain access to an online account to launch another attack.

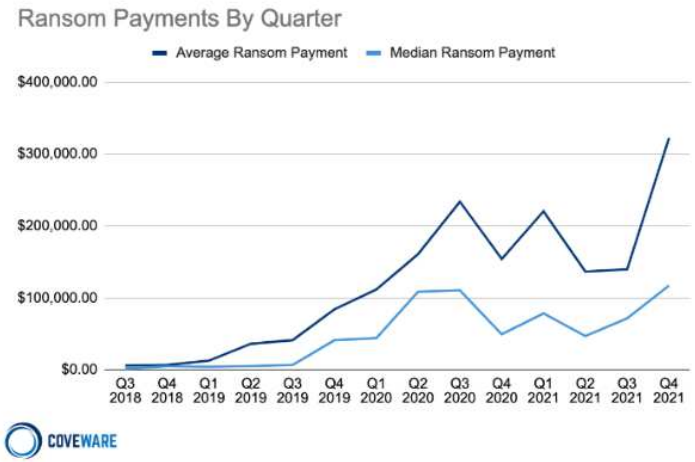
Source: https://www.debevoisedatablog.com/2020/09/30/its-time-to-take-credential-stuffing-seriously/

Business Email Compromise

- BECs are among the most successful and persistent forms of cyber attacks.
- Between 2019 through 2021, the FBI IC3 has received an increase of BEC complaints involving the use of virtual meeting platforms to instruct victims to send unauthorized transfers of funds to fraudulent accounts.
- In 2020, the IC3 reported 19,369 BECs and email account compromise complaints that led to losses of about $1.8 billion.
- Common BECs that companies face include:
  - Executive Email/Voice Fraud
  - Bogus Invoice Scheme
  - Gift Cards/Payroll
- Threat actors are also taking advantage of the Covid-19 situation to make their social engineering schemes more believable.

Source: https://www.debevoisedatablog.com/2020/06/11/fbi-warns-of-a-rise-in-business-email-compromise-scams-tips-for-preventing-and-responding-to-becs-in-remote-work-environments//

Ransomware Attacks



- Ransomware attacks used to be limited to the locking of a company's computer system by encryption software and a demand to pay (usually in cryptocurrency) in order to obtain the key to regain access.
- There is a growing trend of ransomware attacks that includes theft of sensitive company data, with threat of public disclosure.
- Ransomware groups are generally financially motivated criminal actors but some nation states are now engaging in ransomware to raise funds, not to mention attacks driven by non-financial motivations.

Source: https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

Blackbaud

- Blackbaud is a cloud service supplier who suffered a notable ransomware attack, discovered in May 2020. More than 120 nonprofits, including hospitals and educational institutions using Blackbaud's fundraising platform were affected.
- The attackers exfiltrated sensitive data from Blackbaud's network belonging to millionsof donors, potential donors, customers, patients, and other individuals connected with the affected organizations.
- Blackbaud launched an investigation to determine the scope of the incident and affected data. Customers were not notified until July 2020.
- Blackbaud initially claimed that SSNs and user names and passwords weren't affected but had to retract this assertion later.
- As disclosed in its 3Q 10Q, Blackbaud was sued in 23 putative class actions, for alleged harm resulting from the ransomware attack. It also has had to deal with various regulator inquiries, including from the state AGs, FTC, HHS, and data protection authorities from other countries.
- Affected nonprofits had to carry out their own response efforts, and activate notification and communication plans.

Source: https://healthitsecurity.com/news/blackbaud-confirms-hackers-stole-some-ssns-as-lawsuits-increase; https://www.thenonprofittimes.com/npt_articles/the-hack-of-blackbaud-damage-is-still-being-assessed/; https://www.bbc.com/news/technology-54370568


Effective Preparations

Non-Technical Preparations

- **Vendor Engagement**: Who would you call to get help? Outside law firm? Cyber firm? Negotiator? PR consultant? Do you know how much they would charge? Would they be covered by insurance? Better to figure this out ahead of time than during an attack.
- **Sensitive Information in Emails**: Collect and store as little sensitive information as possible. Try to avoid storing credit cards, social security numbers, bank account details, etc. If you do need that data, encrypt it, password protect it, and get rid of it as soon as you don't need it anymore, especially if you are emailing that data.
- **Training**: Train employees on how to spot phishing emails and on avoiding sending sensitive information to personal accounts unless it is password protected.
- **Incident Response Plan**: Have a written plan for all the things that need to be done in a cyber incident and who is responsible for which tasks.
- **Insurance**: Assess cyber insurance options. If you have insurance, understand what is covered, when the insurer needs to be notified, and the vendors they will cover.
- **Passwords:** Require strong passwords that are not being used for other websites. Require mobile phones with organization data to lock quickly, have passwords, and be able to be wiped remotely if lost or stolen.

Non-Technical Preparations (contd.)

- **Tabletop Exercise**: Run a mock cyber attack with your executive team to test incident you cyber attack response procedures, communication strategies, and decision-making.
- **Draft Communications**: Prepare communications for employees, donors, board members, customers and media about an incident, that can quickly be adapted to the facts of the particular incident.
- **Alternative Contacts**: Have a contact list with cell phone numbers and personal email accounts of key persons who will be involved in the response in case the email system goes down in an attack.
- **Third Party Risk Management:** Identify any third parties who have access to you organization's sensitive data and assess whether they are taking reasonable steps to protect that data, and require them to notify you in the event of an incident.
- **Access Controls:** Try and limit access to sensitive information to only those people who need that access to do their jobs. Remember to disable access for people who are not longer working for the organization.
- **Notification Obligation Assessment**: Consider and plan for potential notification obligations you may have arising out of a data breach, including by reviewing government contracts.

Technical Preparations

- Multi-factor authentication for remote access, and access to very sensitive internal systems (know where your most sensitive data lives);
- Patch software vulnerabilities;
- Maintain backups of data that will allow recovery;
- Implement software that can detect malware or unauthorized access;
- Disable Remote Desktop Protocols that can communicated to the Internet or enable MFA for that;
- Tightly control admin/privileged access credentials;
- Delete old sensitive data that you no longer need.

Key Takeaway

- The right combination of steps will be unique to each organization and will depend on the types of information held by the organization, the ways that electronic information is accessed, and the financial and staff resources of the organization.
- Preparedness = Organization-wide Endeavor
- Employees' roles: If you see something, say something!

Example 1: Password Practices

- Easy Fixes
  - Do NOT use passwords used for other accounts
  - Do NOT tell anyone your password
  - Do NOT leave your password on a sticky note
- Illustrative Organization-specific Requirements (Organization's Password Policy/Acceptable Use Policy)
  - All devices used to access the Organization's Information Systems and Organization data must be password-protected
  - Passwords must be at least X characters, contain a capital letter and special character
  - Employees required to change password at least once per year
  - Cannot reuse your last 3 passwords
- If you suspect that your account is being accessed by another individual, you should alert the a designated individual at the organization immediately.

Example 2: Phishing – What to Look For

- Attachments or links from unknown senders
- Sender's email address and domain
- Poor grammar or spelling
- Mismatched URLs (hover, don't click!)
- Emails you did not sign up for/actions you did not initiate
- Requests for personal information
- Urgent notices or requests

Example 3: Email and Mobile Device Hygiene

- Only remove information from the Organization's Information Systems for a business purpose;
- Refrain from using personal email to conduct the Organization's business; limit forwarding of the Organization's emails to personal accounts (with reasonable exceptions);
- Do not automatically forward email messages containing Organization's data from the Organization's email account to non-Organization email accounts;
- Secure mobile devices: cell phones, tablets, laptops etc.
- If you have to use USBs or other removal media storage devices, they should be encrypted.

Example 4: Information Disposal

- Get into the habit of prompt disposal of unused data, subject to legal obligations, e.g. preservation orders
- If you don't need it, get rid of it!
  - Clearing email inbox
  - Shredding documents
  - Deleting electronic documents
- Acceptable means of disposal for PII
  - Shredding
  - Destroying PII
  - Making PII unreadable
  - Reasonable belief it cannot practicably be read or reconstructed

Cyber and Privacy Diligence

- Scope and type of cyber diligence is industry-specific and based the nature of the third-party operation
- Close coordination and collaboration among legal and the advisors conducting technical cyber diligence (if applicable); insufficiency of questionnaires in certain situations
- Key areas of diligence review:
  - Compliance with applicable data protection laws (including cross-border data transfers)
  - History of incidents and investigations or complaints
  - Documented policies and plans that are tested
  - Network and system tests, audits and assessments
  - Vendor management practices and policies
  - Cyber insurance
  - Notification