RE-ISAC Weekly Cybersecurity Report

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

3 November 2017

TLP GREEN: Limited disclosure, restricted to the community. Sources may use **TLP GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share **TLP GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP GREEN** information may not be released outside of the community.

We Three Parties…

IN BRIEF: So many cyber incidents could be prevented by better information sharing relationships with third parties. Third parties can be compromised to impact one's own organization or the organization can be targeted to impact a third party. Additionally, cyber incidents have far reaching implications for clients, residents, patients, consumers, internal team members, partners and suppliers. Most major incidents could have been detected or prevented with better third-party management strategies. Third party management becomes more important and more difficult around the calendar Year's end. Many third parties will be requested to provide event planning, decorating, catering, entertainment, transportation, and even temporary workers to handle the holiday rush while others may be employed to handle end-of-year audit or accounting functions.

KEY TAKEAWAYS & RECOMMENDATIONS:

- No organization is entirely self- contained. Third parties offer necessary (and unnecessary) goods, services, and even personnel that empower businesses to achieve success unattainable by a single organization alone.
- Most cybersecurity incidents involve a third party of affect a third party.
- Third parties and even fourth parties may be more difficult to identify as the supply chain had converged between virtual products and services and real property and tangible services.
- Many organizations struggle to manage open source or free software.
- Even if no money changes hands, any organization with network connections or remote access to corporate networks should be considered a third party for the purposes of risk management.

BACKGROUND. Target experienced a highly publicized incident that extended from gaps in third party management. The Target breach has exceeded $200 million in damages. Cyber insurance paid on the claims, but the coverage fell far short of actual costs incurred (and still being incurred 3 years later). In the case of Target, a third-party HVAC vendor was compromised. The third-party's access to Target's invoicing system was then abused by the criminal actors to

Many organizations suffered from NotPetya ransomware in June of 2017 because malicious code was injected into third-party software used by those organizations. Vulnerabilities in third party web server software (open source software) were exploited to steal information on millions of people from Equifax also in 2017.

Between 2013 and 2015 unauthorized actors obtained information about T-Mobile customers from a server managed by Experian, a third-party T-Mobile used to provide credit application processing. Both firms were named in multiple class action lawsuits.

Multiple restaurant chains have been affected by compromises of third-party Point-of-Sale software and equipment. Sabre Hospitality systems experienced a breach of its central reservations system as announced in June of 2017. So far, Google, Hard Rock Hotels and Casinos, Loews Hotels, the Four Seasons, and Trump Hotels all of whom used Sabre Hospitality for travel arrangements were affected.

Multiple organizations have experienced data exposure due to misconfigured containers or servers in cloud environments. Among them are the Dow Jones, WWE, Deep Root Analytics, Verizon, and Deloitte. The Republican National Committee hired Deep Root Analytics to perform analysis on users to receive advertisements. Deloitte serves many large corporations and government agencies. Perhaps the misconfigurations were the fault of the cloud services users, but perhaps the controls available in the cloud environments were confusing or lacked transparency. Either way, better third-party management may have prevented these incidents and more importantly could have reduced the exposure and harm to others as a result.

Third party management is not limited to services firms, however, don't forget we all use software, web based applications, hardware, networking equipment and security tools. The exploitation of software vulnerabilities plays a role in nearly 90% of malicious security incidents.

Third incidents can result in the loss of intellectual property, the receipt of counterfeit goods, or compromised operating environments. Counterfeit goods can contain malicious software or hardware, malicious features that compromise physical security or safety, can be lower quality items, or can simply rob the brand owner of rightful business and funds. One example can be recalled when counterfeit Cisco equipment was shipped to unsuspecting customers who believed there were purchasing genuine Cisco products from resellers.

MITIGATION. Third parties can include suppliers, partners, government agencies, and organization with whom mergers and acquisitions are planned. If your organization does not already have a comprehensive third-party management process in place, a program should be established that includes the below recommendations. The following steps can help reduce third party risks:

Before Initiating a Relationships

- **Vet Potential Third Parties** – Before engaging a new supplier or considering a merger or acquisition, require the organization to submit a high-level description of how it will protect any data or network connections with your organization. If the organization will have IT assets interconnected with your own, or if the third party will be handling data of critical business importance (or regulated data), a summary of a recent vulnerability assessment and penetration test of the organization's infrastructure should also be required for review.
- **Open the Lines of Communication** – Ask the potential third party what common threats they face, what types of incidents they often thwart or experience, and what types of threat actors they face. Share this same information with the potential third party.
- **Assess How the Relationship Impacts Business Risk** – Does the relationship add additional risk? Is the cost of mitigating that risk worth the value added by the third party? Can the third party mitigate the risks business with you might add to their risk posture?

Negotiating an Agreement

- **Set Clear Expectations** – Provide the third party with a list of all regulations, frameworks, and policies with which they must comply. Include compliance with these materials in the contract. Include contract provisions that explain penalties for failure to comply and how compliance will be audited. More specifically contracts should include the following requirements:
    - All vendors must review, sign, and maintain compliance with security requirements and acceptable use policies.
    - Require vendors who transmit or store sensitive data to encrypt it both at rest and in transit.

    - Require vendors to provide immediate notification of any data breaches or cybersecurity incidents that may impact your organization, your clients, or your customers.
    - Require that vendors perform comprehensive background checks on their employees. These background checks should be performed regularly, preferably on an annual or bi-annual basis.
    - Require that all software and systems used by vendors to access your networks or sensitive data are running antivirus software and kept up-to-date with the latest security patches.
- **Review Insurance Policies** - Both parties should review insurance policies regarding cyber incidents. Don't forget that cyber incidents may not be limited to data breaches. Business impact could occur if a third party become inoperable from an act of nature, hardware failure, or human error. Insurance policies may cover third party incidents. Your third party should also review their own insurance coverage. Contracts should require the third party to carry enough insurance coverage to mitigate risk to themselves as well as you and your customers in the event of a cyber incident. Insurance coverage may also inspire additional contract language regarding liabilities or indemnification in the event of a cyber incident.
- **Specify Service Level Agreements** – Contracts should spell out explicitly the minimal expectations for service, uptime, frequency of response, and minimal amount of response times for services specified. These may not be necessary for all third parties, but should be in writing for those that do perform critical services or provide critical asset support.
- **Specify Contingency Arrangements** – if a product is not performing, requires repair, or has become inoperable, who is responsible for the service or repair? Who and how often will the product be serviced? Will there be software or firmware updates? Who is responsible for security vulnerabilities? Can the product be replaced or exchanged? How quickly and who pays for shipping?
- **On-Site Work** – If third party personnel require on-site access, how with this be managed? Are third party personnel permitted to take company data or equipment with them upon leaving?
- **Determine Payment and Communication Channels in Advance** – Will communication occur via email, a proprietary portal, phone call, or in person meetings? How will payments be made, and invoicing be conducted. These arrangements should be shared with others. How will changes to these arrangements be communicated (they should not be limited to email). By determining these details in advance, BEC and Wire Fraud scammers will have less success in social engineering your accounts payable personnel to direct funds via a different procedure or to the wrong account.

Review Existing Relationships

- **Bring Existing Agreements into Compliance** - On an annual or bi-annual basis, existing agreements must be reviewed to ensure compliance with new laws, regulations, and other security and privacy obligations.
- **Review Data and Connections** – Both the written description of data shared with third parties and any connections and accesses they have in your organization should be reviewed periodically. Do you still need to share the same types and volume of data? Does the third-party still require the same level and breadth of access. Technical reviews of the data and connections should also be conducted to ensure only those needed for the third party to perform its duties are provided. Technical reviews should include audits to ensure that data is appropriately handled, secured, and destroyed or returned as appropriate and that any connections and accesses are used appropriately and only when needed.

Keep the Lines of Communication Open and Include Third Parties in Risk Prevention, Preparation, and Incident Response Planning

- **Include Third Parties in Exercises**
- **Continuously Share** Information about threats, incidents, and anticipated adversaries with third parties.
- **Encourage Third Parties to Share** the same information with you**.**
- **Keep Third Parties Informed** of any changes to regulations or legislation that may affect their obligations as part of the agreement.

We are all a Third Party to Someone

The New Jersey Cybersecurity and Integrations Cell Recommends the following for each of us to remain responsible third parties to our own clients:

- Implement a comprehensive vendor management program, beginning with audits of all current vendors.
- Prior to implementing new hardware or software products into a production environment, fully vet the product to ensure it works as expected in a test environment.
- Leverage trusted third-party security review resources including the National Information Assurance Partnership,
- FedRamp and Cloud Security Alliance CSTAR certifications, etc.
- If possible, conduct source code reviews of all third-party software used within your enterprise.
- Establish security controls and regularly audit vendor access to your networks, systems, and sensitive data.
- Apply the Principle of Least Privilege when creating user accounts for vendors and regularly monitor and audit accounts for abuse and privilege escalation.
- Require two-factor authentication, the use of a VPN, and/or apply IP address whitelisting for remote access to all systems and portals that contain sensitive data.
- Limit or eliminate the transmission or storage of unnecessary customer and client information.
- Maintain awareness of all compliance mandates, security standards, and reporting requirements and update policies and procedures to incorporate changes as needed.
- Ensure that all security requirements, including acceptable use policies, are clearly defined in vendor contracts.
- Implement proper network segmentation to protect systems and data from unauthorized access by vendors and other external threats.
- Block traffic to unneeded ports both at the network perimeter and on internal systems, servers, and firewalls.
- Disable, delete, or block the use of unneeded remote access tools such as PsExec, Microsoft Remote Desktop,
- TeamViewer, VNC, LogMeIn, etc.
- Whitelist authorized applications and proactively block the installation and usage of unauthorized software.
- Consider implementing a data loss prevention (DLP) solution that includes monitoring of all egress traffic for unauthorized data exfiltration.
- Follow established change management processes.

Additional Resources can be found at:

https://csrc.nist.gov/projects/supply-chain-risk-management/publications

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

https://www.nist.gov/sites/default/files/documents/itl/csd/NIST_USRP-Boeing-Exostar-Case-Study.pdf

https://www.sans.org/reading-room/whitepapers/analyst/combatting-cyber-risks-supply-chain-36252

https://www.tag-cyber.com/annuals/Volume_1_-_TAG_Cyber_Security_Annual_-_Fifty_Controls.pdf

https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

https://www.fdic.gov/news/news/financial/2008/fil08044.html

https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf