JFX, LLC
Cybersecurity Consulting

# JFX Cybersecurity Briefing: Cybersecurity Threats

October 2024

This briefing reviews common cybersecurity threats and how to protect against them, incorporating information from the FBI, cybersecurity companies and insurance groups.

## Vendor / Supply Chain Attacks

*Risks*: Many organizations depend on external vendors to perform what in the past would have been internal business functions, such as Accounting and HR services, both of which require access to confidential information. There also has been a fundamental shift to cloud hosted services and data storage, with fewer companies managing their own data centers. Cybersecurity vulnerabilities of those vendors or vendor managed systems are involved in many cybersecurity breaches.

*Protections*: Review which vendors have access to your critical systems or confidential data, and know which perform business critical functions. Ask what controls those vendors have, and - to the extent possible - limit their access to systems and data. Make sure you understand what responsibilities you have as a user for setting and monitoring cybersecurity controls, e.g., requiring MFA and monitoring user activity. In terms of business continuity, identify the operational impact if a vendor is not available, and plan the steps you would take to mitigate or recover from that outage.

## Business Email Compromise Attacks

*Risks*: “BEC” attacks impersonate real business relationships, often incorporating information gathered through social engineering, social media or compromised emails. Often claiming urgency, these messages convince firms or people to make or re-direct payments to hacker controlled bank accounts. With quick notification to the FBI (IC3) or law enforcement payments sometimes can be recovered, but once money has been redistributed it often is gone for good.

*Protections*: Establish and enforce payment procedures to separately confirm any new or changed payment instructions, especially if they say they are urgent. Do not use the same communication method that made the request. Note, attacks may target holidays, when usual staff often are on vacation and those doing payments may have less familiarity with normal activity.

## Vulnerability Attacks

*Risks*: Especially for externally facing / connecting systems, e.g., web portals, automated scans can quickly detect vulnerabilities in old or misconfigured software. Once hackers get access, they have well established methods to gather system information and capture more powerful user credentials, moving across systems and networks for maximum access.

*Protections*: Update software to run current versions, which should include most recent security updates. Review device and system configurations and turn-off unnecessary functions (such as remote desktop access). Run vulnerability scans on both external and internal systems and prioritize remediation to those with the highest business risk. Limit accounts with system administration rights, and only use those permissions to do the work that requires them. Turn on MFA where possible.

## Ransomware Attacks

*Risks*: If a hacker is able to get system access through a vulnerability, or can get a user to click on and run a corrupted link or file, ransomware can encrypt data, with criminals demanding payment to provide a decryption key. A common extortion variation is to export data first, with a threat to release it or to disclose security violations to regulators.

*Protections*: Keep off-line copies of both data and software (operating system, installed programs, etc.) needed to recover a corrupted device . Encrypt confidential data where possible. Test recovery of data and systems, both to make sure you have what you need to recover and also know how to do it (including how long it takes).

### Threat Actors, aka, Cybercriminals

*Risks*: Cybercrime is very profitable, and risks of arrest and punishment are very low. In some cases hackers are affiliated with or tacitly supported by hostile governments. Like other service businesses, criminals now specialize, so a ransomware attack may include a hacker licensing the ransomware, buying system access, and outsourcing ransomware extortion payments.

*Protections*: Participating in threat information sharing groups improves individual and collective abilities to identify and respond to attacks. Coordination with law enforcement is another critical step, ideally using contacts established prior to an attack. Cybersecurity needs to move beyond defining success as self-protection, to include capturing and sharing information about attackers so law enforcement can arrest, convict and punish cybercriminals, the same deterrence for other types of crime.

JFX, LLC is a cybersecurity consulting firm that helps businesses identify and manage their cybersecurity risks. For more information contact info@jfxllc.com