What the Recent Cyberattack Means and Ways Businesses Can Protect Themselves

October 24, 2016

The unprecedented cyberattack on October 21, 2016, which crippled many of the Internet's most widely trafficked sites, should be a wakeup call for businesses about the potential for hackers to weaponize common Internet-enabled devices and cripple businesses.

What Happened?

The cyberattack was caused in part by malware directed to more than 10 million Internet-connected devices, including DVRs, thermostats and closed-circuit video cameras. It caused a distributed denial-of-service attack (*i.e.*, service interruption) that hit in three waves. Dyn, an Internet services company that directs Internet traffic, reported that the attack hit *all* of its 18 data centers globally. Early reports show that the disruption may be responsible for up to $110 million in lost revenue and sales. Perhaps most troubling is that the group claiming responsibility said the attack is merely a dry run for much larger attacks.

Cybersecurity is now a business necessity because breaches are anticipated to multiple exponentially as more IoT devices make their way into homes and businesses.

The Magnitude of Cyberattacks Will Rise as the "Internet of Things" ("IoT") Continues to Evolve

The IoT is a giant network of Internet-connected "things" that include everything from cellphones, manufacturing equipment, utilities, home appliances (coffee makers, refrigerators, lamps, etc.), cars, wearable devices, technology-enabled clothing and anything else that can be imagined. Cisco states that 15 billion IoT devices are in use today, and there will be 50 billion IoT devices by 2020. Never before have so many Internet-enabled devices been in our homes and workplaces, and in the coming years, it will change the way we do business and engage in everyday activities.

Security analysts report that many of these devices do not have appropriate security features, making them a prime target for hackers. Unlike well-established computer servers and smartphones with robust security features, many of the new devices—which are often designed for a specific purpose, at a lower price point, and with a limited product life—have not been fully vetted and their makers may not always engage in rigorous security testing.

Steps Businesses Should Consider to Protect Against the Inevitable Breach

Cybersecurity is now a business necessity because breaches are anticipated to multiply exponentially as more IoT devices make their way into homes and businesses. With the increasing number of devices being connected daily, businesses can no longer delay in preparing for the inevitable breach.

Below are steps that you should consider for your business to ensure you are ready when on the receiving end of a cyberattack:

- Ensure security gaps are identified and remedied *but* also ensure that outside legal counsel engages technology consultants on your behalf and that legal counsel works directly with consultants. Doing so may enable businesses to assert attorney-client privilege over the results of technology audits and investigations;
- Review and update your security program and policies to ensure they are comprehensive and up-to-date;
- Develop a bring your own device ("BYOD") policy to address the types of devices employees may connect to your computer systems;
- Update privacy policies to ensure they are accurate and appropriately convey the business' collection, maintenance, use and security of consumers' and employees' personally identifiable information;
- Conduct cybersecurity and privacy training for employees. Many breaches are a result of an employee's mistake or negligence, and policies and procedures are not effective if not known and practiced by the entire workforce;
- Develop an incident response plan that outlines in detail your business' response to a cyberthreat to ensure you are prepared to act promptly;
- Run a mock data breach exercise to practice implementing your incident response;
- Review and update contracts with third-party vendors to confirm that they are engaging in appropriate security measures to protect your key data assets and to update limitation of liability and indemnity clauses for cybersecurity events; and
- Review relevant insurance policies and determine what your insurance covers and to what extent. Insurance coverage for cyberattacks and data breaches varies widely from policy to policy, so simply confirming that you have "cyberinsurance" may leave you exposed.

Technology is advancing rapidly, and businesses no longer have the luxury to address cybersecurity at their convenience or engage in limited security initiatives. Taking these proactive steps may help businesses be prepared when the "big one" hits.

For Further Information

If you have any questions about this *Alert*, please contact Sandra A. Jeskie, any of the attorneys in the Information Technologies and Telecom Practice Group, any of the attorneys in the Cybersecurity Response Team or the attorney in the firm with whom you are regularly in contact.