2022 CLM Construction Conference
Sept 21st – 23rd 2022
San Diego, CA

Easiest Catch: Don't Be Another Fish in the Dark 'Net

You've read the headlines. Unfortunately, the question now is not if your information is going to be accessed or stolen, but when. To inform the attendees of current developments in the digital underground as well as provide realistic advice for cyber protection, Chris Lester will be discussing recent high-profile cybercrime events, including website breaches impacting a variety of organizations and sectors. Chris will discuss particularly dangerous types of threats that might affect organizations involving the Dark Web, the Internet of Things, and phishing.

I. Types of Threats to Cybersecurity Posture

Unintentional

Unintentional threats may include an employee falling prey to a phishing scam, a browser exploit, or some other kind of hack that compromises the data to which they have access. Wi-Fi attacks and the possibility of having a device stolen are also very dangerous and common, especially as people spend a greater amount of time working remotely. I once had a frantic phone call from a young attorney who had left their laptop in their car overnight. The next morning it was gone. Luckily, the laptop had been encrypted, so the potential for damage was somewhat minimized. However, unintentional threats pose great risk and can be very costly to a firm financially, reputationally, and operationally. Typically, diligent employee education programs and regular training (especially following regularly scheduled security assessments) can improve defense strategies and establish reliable reporting mechanisms when unintentional security issues arise. Communication within organizations is key when it comes to responding to these instances head on.

Malicious

Conversely, malicious insider threats are impervious to training efforts and may prove more severe if an employee has extensive IT knowledge. A consistent trend I have observed in conducting routine organizational security assessments is that management issues with access controls are common. When too many people have too much on-demand access to too much information, there is more room for things to go wrong (and more seriously wrong). The more access a disgruntled employee has, the more successful their attack is going to be. In one unfortunate instance, a concerned firm contacted me with the suspicion that a former employee was continuing to access their systems remotely. Furthermore, it was suggested that perhaps this employee had also been sending confidential information to a private email account in the months leading up to their departure, with the intent to begin a competing firm. The person was also suspected of downloading data beyond the scope of their own active cases to a USB device. Upon reviewing the details of the case, it turned out that this firm had not collected the employee's devices upon their termination, and that the employee had continued access to the firm's confidential client and case information. Despite unusual network activity leading up to the former employee's departure, nothing was done to discover what was being downloaded en masse, and the employee's access controls remained the same even after they had announced their intention to leave the firm.

II. Internet Of Things (IOT)

Smartphones are probably the biggest storehouses of our personal information that we utilize daily, and for that reason, they are probably the devices that transmit the most data about us as well. But now, internet-connected devices can include everything from your thermostat to your car to your refrigerator. These devices often feature a large range of multimedia capabilities that extend far beyond their technical use. Microphones and cameras are common elements of some of our internet connected devices, not to mention other more advanced technologies such as GPS and voice recognition. To further confuse things, the average consumer may not know which devices have which features, especially since something as simple as a washing machine may now be equipped with exceedingly advanced technology.

Compliance with technical control standards can never override the human element of security. Organizations can support security, budget appropriately, pursue compliance, assure customers and clients of their attention to latest requirements and best practices—and still be insecure. Accounting for the human element requires interactive, regular training that considers each employee's unique role in contributing to an organization's security culture. While every employee is responsible for security, different roles and responsibilities require personalized education. Additionally, training for new technologies—as well as an organization's incorporation of the Internet of Things—should always be provided across departments. Attorneys are held to an especially high standard when it comes to the information they protect. According to the American Bar Association's Formal Opinion 477R, "a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.”3 The reasonable efforts required by the legal community to prevent data breaches necessitate thorough education that takes the firm’s specific needs, and types of data, into account. Compliance with policy is only worthwhile when upheld by a culture of security that acknowledges the unpredictability of a changing threat landscape.

III. Phishing

Anything shared online can potentially be used to harm a firm financially, operationally, or reputationally. Threat actors tend to have financial gain as their primary motivator. Ransomware and phishing attacks are typically examples of money-driven cybercrime. Hacktivism is more personal, and the mindset of a hacker with a social or political agenda may have an impact on how an attack is conducted. Apart from the team effort that groups like Anonymous can marshal, hacktivist attacks may be more tenacious than your average cybercrime venture, and government entities may be particularly targeted. .

Access controls are a critical piece of an organization’s overall security posture. Limiting access to critical data, systems, and networks is a surefire way to mitigate some of the potential risk. The more an employee can access, the greater the liability that employee poses in the event of a compromise. Restricting and auditing access controls do not make employees immune to spear phishing attacks, but these measures limit the damage when employees become victims. Second, training and education are always going to strengthen organizational security, but employees should be reminded that avoiding hastiness is always important when dealing with digital communications.

It is important to communicate to employees how personal information will be requested, and to establish that following up in person is encouraged (or required) when a request for personal information has been received. While email is the standard phishing method, it is important to remember that phone calls and texting can also be used to gather information. If anything appears suspect or out of the ordinary, make sure that reporting procedures are in place and that all employees know the designated communication channels. Taking a moment to slow down before acting on a request may make all the difference.