ES&A
A LAW CORPORATION

MEMORANDUM

To: ES&A Clients and Friends
From: Anna Elento-Sneed, Esq.
Sam Sneed, Esq.
Date: 10/30/2015
Subject: **Cybersecurity and Cyber-Safety: Be Afraid, Then Be Prepared**

Cybersecurity is often thought of as a problem for the high tech and defense sectors. In honor of Halloween and Cybersecurity Awareness Month, we've brought you three examples of the horrors that can unfold when an organization fails to take simple measures to protect itself.

Horror Story 1: "We've got company!"

Most offices today use physical access control systems to limit the persons who may access different areas of a facility, often using key cards or number combinations to unlock doors and elevators. This presentation from DEFCON 23 in August of this year demonstrates just how easy it is to break into these systems.

Control units are often installed without changing default passwords, using factory-installed locks, and connected to an organization's network to allow for remote control. Accessing a control unit located in a publicly-accessible area can require as little effort as searching online for the model's default passwords or master keys. Control units in more secure locations may still be remotely accessed via the internet. Depending on the software used and its configuration, an attacker may use default passwords, use a "brute force" attack[1] to crack the password, or bypass the system altogether. Once an attacker has access to the control system, he or she may lock or unlock any connected doors at will. Depending on how robust the system's tamper monitoring is, administrators might never know when or how it happened.

Why You Should Be Concerned: Networked devices offer huge savings in time and energy, but not all have comprehensive or effective security measures. Even a well-designed system may be rendered useless

[1] Brute force attacks used for password cracking use a guess-and-check method to quickly generate and test possible passwords. These can typically be accomplished with short, simple lines of code, many examples of which can be found online. How quickly a password is cracked depends on the length and character space of the password. Character space is the number of possible characters that may be used – for example, numbers have a character space of 10 (0-9), and upper and lower case letters have a character space of 26 each. A 3-character password using only numbers would have 1,000 possible combinations for a brute force attacker to attempt, while a 3-character password using numbers, uppercase and lower case letters would have 238,328 possible combinations. Therefore, the longer the password and the larger the character space, the harder it is for an attacker to crack.

if administrators do not monitor access to the system or change default passwords. Useless locks mean your physical safety is at risk.

While physical access control systems like door locks are just one example, the same problem exists for every control device on your network. The "Internet of Things" has enabled remote access to everything from the electrical grid to tea kettles.[2] The more critical a network device is to your operations, the more important it is that comprehensive security measures are in place to protect it.

Ways to Protect Yourself: Evaluate your network and connected devices. Below are a few questions to get you started:

1. What systems in your organization are critical to your operations and safety? E.g., gates and doors, CCTV cameras, automated machinery, document management, email, etc.
2. What devices control and secure your critical systems?
   a. Are they accessible to the public?
   b. Are they connected to your network?
   c. What security features do they include? Have default access codes been changed?
   d. Are they monitored for intrusions? By whom?
3. How secure is your network?
   a. Who is allowed to access the network?
   b. What non-critical devices and systems access your network?
   c. How strong is your password? How frequently is it changed?
   d. Do you have an Acceptable Use Policy for network users?

Horror Story 2: The Business E-mail Compromise

In January of this year, the FBI issued this public service announcement on the "business e-mail compromise" scam, which targeted businesses that regularly performed wire transfers. Scammers first identify employees, supervisors, and/or third parties involved in wire transfer transactions. Next, supervisors' or client's work and travel patterns are tracked using publicly-available information (often social media) and their email accounts may be hacked. Using this knowledge and/or access, scammers then convince an employee responsible for directing wire transfers to authorize a transaction into the scammer's bank of choice, often calling at inopportune times during the day or sending an email that appears to come from the employee's supervisor or client.

Why you should be concerned: Last year the FBI documented over 1000 U.S. victims who lost over $170 million dollars combined. The banks used by scammers are often unaware of the activity and/or are outside

[2] A recent report found that smart tea kettles contained a vulnerability that allowed attackers to steal the passwords of the Wi-Fi networks they used.

of the U.S., meaning recovering lost funds is extremely difficult. Even if your organization does not use wire transfers, similar scams have been documented for other types of transactions.

Ways to Protect Yourself:

1. Set up training for employees and managers on cybersecurity and online safety.
2. Evaluate your procedures for authorizing payments and how much information about these procedures and employee work duties and schedules is available on social media, company websites, and other publicly-accessible mediums.
3. Use a 2-step verification process. When a request to release any funds is received, an employee should verify the request in a *different* medium.
   Example: If Employee receives an email from Supervisor directing payment to Outside Party, Employee should call Supervisor to confirm. If Employee must use email, Employee should create a new message or use "Forward." Employee should *not* click "Reply."
4. Immediately delete spam email. If you receive an unusual email – *even if it appears to be from a familiar sender* – do *not* open attachments or links. First verify that the email is from the purported sender via phone or other method of communication.
5. Red flags that warrant follow-up via phone or other method of communication include:
   a. Sudden changes in business practices, especially if related to the transfer of funds or property;
   b. Sudden requests to direct communications to a personal email or unfamiliar person; and
   c. Requests to take action quickly or secretly.

Horror Story 3: A Visit From a Hacktivist

Earlier this month a former Reuters journalist was found guilty of helping the hacktivist group Anonymous[3] access and alter the LA Times website.[4] According to the indictment, several months after he was terminated the employee gave login credentials to self-identified members of Anonymous over an IRC,[5] then told them to "go f--- some s--- up." A few days later, the content management system for the LA Times website was accessed to alter a published news story.

Why you should be concerned: Employees access, interact with, and manage your systems on a daily basis. Attackers do not need advanced technology to gain access or control of an organization's systems –

[3] "Hacktivist" is a portmanteau of "hacker" and "activist." Groups often target high-profile or politically controversial organizations and utilize a variety of methods to disrupt or deface their victims' operations. Hacktivist groups are often decentralized, loosely-affiliated groups of anonymous individuals. Well-known examples include Anonymous' distributed denial-of-service attacks and fax spamming the Church of Scientology, the Anonymous hack of KKK social media accounts and threats to reveal identities, and the LulzSec denial-of-service attack on the CIA website.
[4] See Journalist Linked to Anonymous Found Guilty of 5 Federal Counts of Hacking.
[5] Internet Relay Chat (IRC) is an online system for sending and receiving messages in real time. Discussions may be held between two or more people and are often created around a common subject.

many times they simply ask to be let in. Checks and balances in access rights must be established to prevent or mitigate the effects of an employee who does not follow established access procedures.

Similar security breaches can occur even when employees are not actively trying to grant unauthorized access to your systems. Successful scams often use "social engineering"[6] to manipulate unwitting victims into giving up critical information or act against established policies.[7] As with any other job functions, a lack of training and supervision – or in the example above, comprehensive out-processing – can put your operations at risk.

Ways to protect yourself:

1. Have an Acceptable Use Policy that clearly communicates how and when employees may access your organization's systems.
2. Set up training for employees and managers on cybersecurity and online safety.
3. Evaluate how your organization manages access to its systems.
   a. What levels of permissions exist for each system?
   b. What are your procedures for granting and monitoring access?
   c. What are your procedures for modifying or revoking access?
4. Signs that an outside contact is attempting to use social engineering to manipulate your actions include:
   a. Requests for information that he/she should already know or should not have access to;
   b. Unusual persistence or resistance to your attempts to terminate a conversation or email/call back at a later time;
   c. Requests to direct communications to an unfamiliar phone number or email address; and
   d. Requests to take action quickly or secretly.

[6] "Social engineering" is a broad term for actions or statements intended to influence a victim into performing a desired act or divulge certain information. For more information and examples, see http://www.social-engineer.org/framework/general-discussion/ and https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529.

[7] In the last year alone, Microsoft has received over 175,000 customer complaints about the common "tech support scam" in which scammers claiming to be technical support for a major company convince victims to divulge credit card or bank account information. For more information on this scam and social engineering, see http://news.softpedia.com/news/microsoft-received-over-175-000-customer-complaints-regarding-tech-support-scams-493573.shtml and https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_en.pdf.