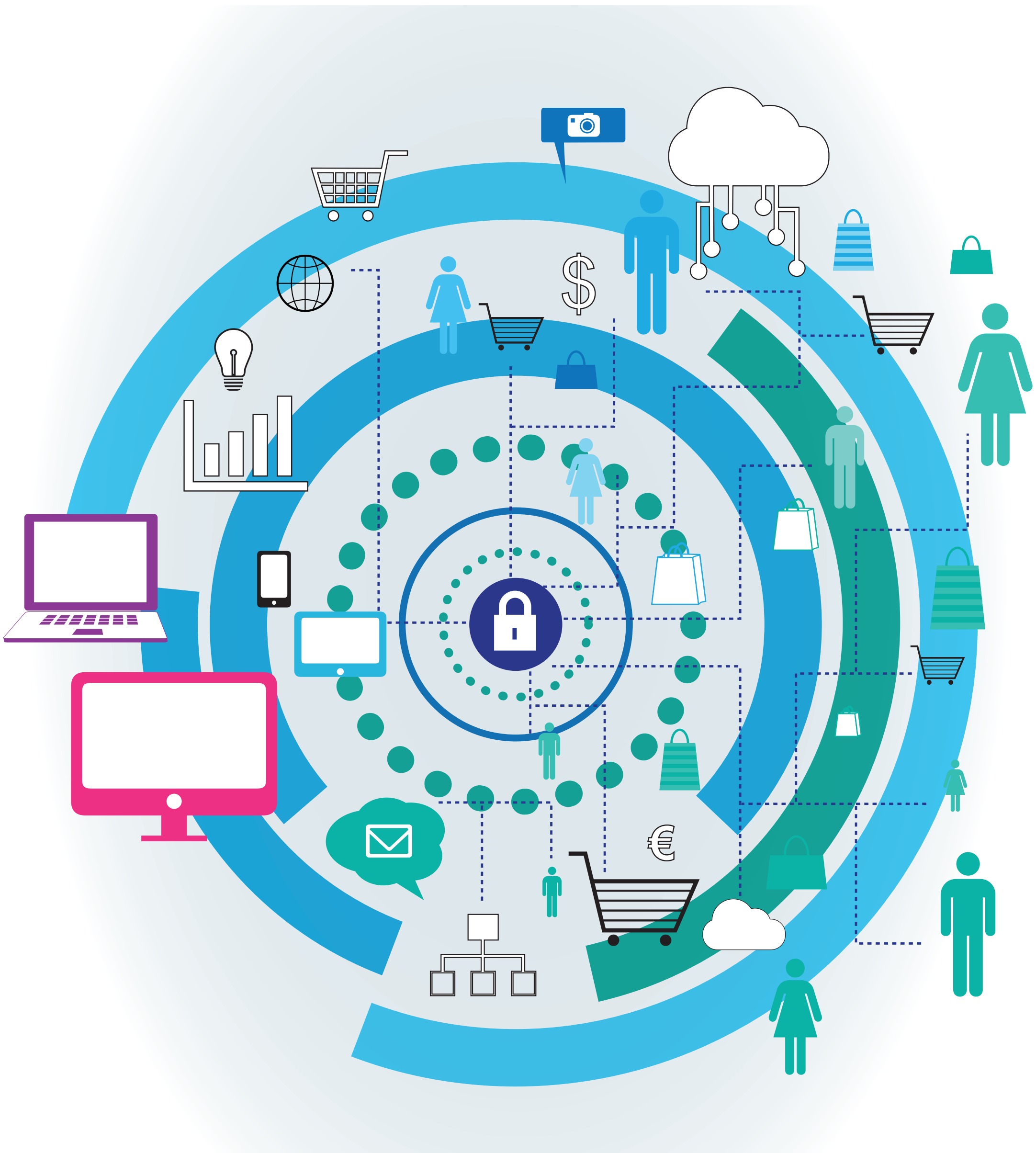

INDUSTRIAL INTERNET OF THINGS AND CYBERSECURITY

Howard W Penrose, Ph.D., CMRP

You get up one cold morning, check the status of your vehicle and then start it while eating breakfast. Tire pressure is good and it's still under warranty – but there is a recall. You select the button on your smartphone and set an appointment with the local dealership. Before you finish getting dressed, you check the status of your office to ensure that the electronic thermostat has changed to the correct temperature and you take a quick peek at the security cameras, from your smartphone, and see that one of the managers has not arrived yet. The phone rings. He is trying to enter from the back door and has forgotten his key, so you open the appropriate mobile application to unlock the door. You finish tying your shoes, go to the garage and climb into your already-warmed up vehicle. You then realize you forgot to turn off some lights and the heat in the house, so you go onto your smartphone and make the necessary adjustments.

At the office, you log in and take a look at the status of the plant. A critical pump is trending up in vibration and a few drives tripped overnight and were reset. Work orders to evaluate the conditions were issued through the computerized maintenance management system (CMMS) and appear to be in process. You take a sip of coffee and check the overall plant KPIs and note that the automated maintenance monitoring programs are working reasonably well. There were a lot of complications as the controls were installed, but energy costs have been dropping and plant availability is up. A news item catches your eye in the corner of your browser – something about the federal government paying a computer consultant to hack iPhones and the potential implications.

An email comes in from the local utility about a past due bill. You're surprised since your bills are paid automatically through your bank and credit card. However, another credit card theft issue came up recently. Maybe you didn't receive a new card or warning. You open the email that's difficult to read on the small screen. You select the link to the website listed on the email and it takes a while and nothing shows. You put it off until later.

A few hours later, the temperature in the office is pretty chilly. It appears the thermostat has been turned off. However, the team can't focus on that because all of the production lines went down on high vibration alarms. You receive a call from IT, it's fuzzy, but you hear something about *urgent* so you head to your car to drive to the off-site IT department. You discover your car won't start. A call from your bank, while you are contacting the vehicle service, informs you that all of your credit cards and bank accounts have been compromised. You get another call to discover that a primary compressor that keeps the plant operating properly has over sped and is severely damaged. As things continue, you get another call from IT saying your Outlook account sent an email with a malicious attachment to everyone on your contact list.

Is this scenario realistic? Absolutely.

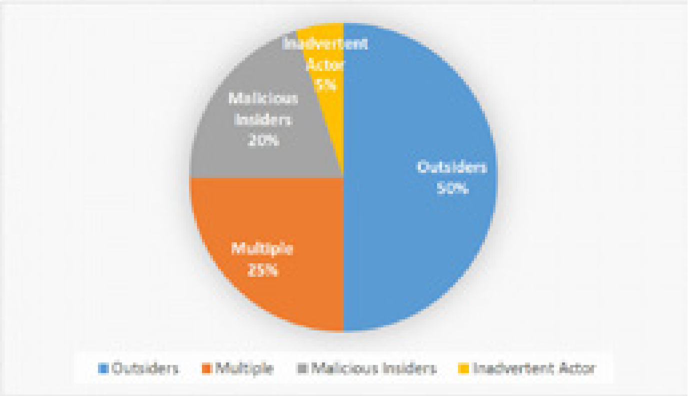

Figure 1: Categories of Attackers (IBM 2013)

The Target store hack that stole some 40 million credit card numbers and customer information was traced to a third party mechanical contractor, one of their HVAC contractors, who monitored heating, cooling and refrigeration for roughly 1,800 Target stores. The complex cyberattack focused on the weaknesses of the third party contractor and gained access through their billing/contracting communications system following the opening of a malicious email to someone within the company. The email installed a 'worm' that went past the firewall and, once in the system, enabled the cybercriminals to check on the background of the administrators. They figured out one password within a week and then placed a malicious software program that infected all of the registers at the stores. The software, written by a 17-year-old Russian hacker, would collect credit card and personal information and send it out as part of an information packet each day for almost eight weeks.

CYBERSECURITY

Since the 1980s, we've been entertained by movies and television programs that warn us of cybercriminal activity. Much of these plots were considered science fiction at the time. How could someone control systems via the internet? Since 2000, however, systems started becoming available that could allow businesses and homeowners access to information and operate systems via computer and, later, smartphone. As we move more into 2016, the term Internet of Things (IoT) has become more prevalent as a greater number of systems begin to come online for information or performance.

Terms that are quickly becoming common vocabulary include *cybersecurity*, *cybercriminal*, *cyberphysical*, *cyberinformation* and *cyberattack*, as well as the *Industrial Internet of Things (IIoT)*. Governments and large companies are putting together cybersecurity strategies to protect themselves from costly impact from cyberattacks by malicious governments and individuals.

With the convenience of the internet and devices coming onto the market manufactured world-wide and installed onto equipment on almost a daily basis, and the push by end-users and manufacturers of the technology to get to market first, what could possibly go wrong?

In one test, 'white-hat' hackers, those who perform hacks to find security issues, discovered that a number of network-connected light bulb (smart bulb) technologies can be used to expose Wi-Fi passwords and credentials to anyone in proximity of the devices. In another incident, smart devices had malicious code present within their system so that when they were plugged in, information on the related network was broadcast to the hackers that installed the software, placing them firmly behind the smart device customers' firewalls. There are other numerous cases of low-to-no security devices being installed on secure systems creating cyberholes that can be exploited by 'black-hat' hackers, those who perform hacks in order to attack a system with malicious intent.

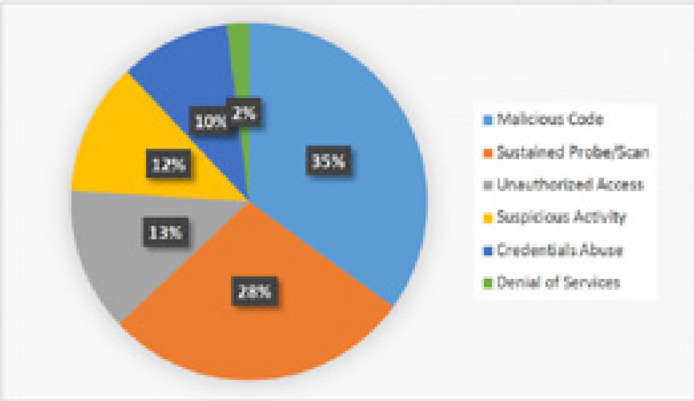

Figure 2: Categories of Incidents (IBM 2013)

A significant amount of coding systems that are used to develop smart devices and connect them are made in such a way that novice developers can work on and create them easily, which indirectly makes it easy for cybercriminals to hack into them. Ease of development usually means ease of access to your system.

To make matters even more serious, while there are many IoT devices that have weak security, regardless of manufacturer, there are many users who are used to plug-and-play services and will most often leave the default password or security protocols on the devices. How often do we read the instructions, after all? Once these are set up on a network, there are very easy ways to find them.

In effect, you are as secure as the weakest point in your system.

FINDING SECURITY HOLES – ACCESS TO YOUR SYSTEM

It's a good thing that your facility is not as easy to find as the local utility. After all, Southern Company's CEO stated, "Can an attack on a small municipal utility cause a widespread blackout? No. What you do there is manage it. Now, somebody getting into the energy management system of Southern Company – avoid like crazy. The cost of blowing this thing is awful, so you have to get it right."

SMRP started working with the Department of Homeland Security (DHS) and supporting their cybersecurity efforts through our Government Relations program in 2015. The rising application of IIoT devices within our member companies makes this a particularly important issue. During our participation, we were exposed to a search engine called Shodan.io. This search engine looks for systems, such as IoT devices, webcams and systems that are connected to the internet and provides detailed information on the system as well as the ability to access those systems anywhere in the world. Developed for the purpose of testing the vulnerability of systems, it is just as available to cybercriminals. While reviewing the system, we had access to SCADA systems, security cameras, control systems, etc. within minutes, including all of the information associated with those systems, and model and serial numbers of the exposed cyberphysical (ability to manipulate) systems. We stopped short of attempting to enter in default passwords to see if we could gain control of several systems. However, we did get an eye view of the status of those systems.

What's quickly discovered is that exposed systems are available for relatively quick access by a cyberattacker. However, we can consider that these systems are installed securely by contractors – right?

I've been involved in discussions and have overheard other conversations during travel and visits where the 'tricks of how to bypass IT' to install a convenient system are discussed. These are not usually concepts, but actual strategies and tactics that are put to use. The end result is a system that bypasses security firewalls and may expose your company's network to cyberattack. What happens when a personal computer or laptop is plugged into a system that is secure from the internet, but has Wi-Fi connected to a system that is directly connected so that the user can access email?

Switching to a new smart device can also have consequences. For instance, if a smart device fails and a new one is installed, how is it evaluated to determine its weaknesses? Does the person installing it have the necessary background or experience to ensure that it is installed correctly and securely?

Besides, my company has no reason to be attacked.

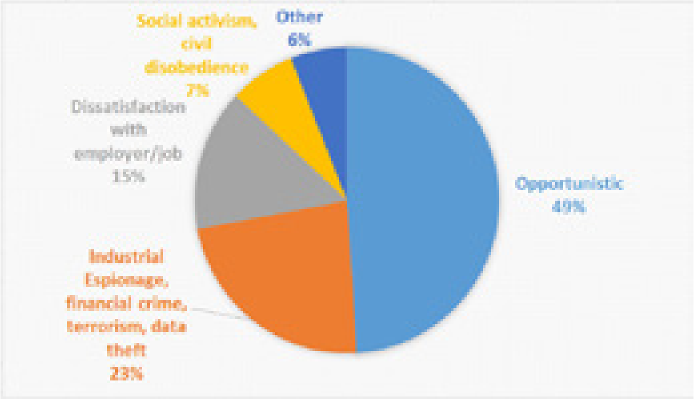

Figure 3: Attacker Motivation (IBM 2013)

More often than not, there is no reason other than that the opportunity is there (49% opportunity) or an employee/contractor is getting back at the company (15% employer/job dissatisfaction). With the present level of access to the internet and, as observed within social media, people acting out anonymously or in ways they would never do in person, the chance that a casual or purposeful attack on a company has increased dramatically. In 2014, IBM published that an average company is cyberattacked 16,856 times per year with a majority of reasons being misconfigured systems or applications.

HOW TO AVOID CYBERATTACKS – OR SURVIVE THEM

As the IoT (or the marketing term IIoT) provides a level of capability that will improve company competitiveness and system availability through monitoring and plug-and-play networking, it is a necessary move forward in technology. However, there is absolutely no doubt that cybersecurity is an issue with the application of these systems.

While the federal government is working toward ways and means to manage cybersecurity issues and cyberattacks in the military, public and private sector, much of the work is focused on defense of larger companies that would have significant impact on the economy. Smaller companies that provide services and consulting to these organizations are not the present focus, which may result in creating vulnerabilities to all parties involved.

At a previous employer, a simple email with the subject line "I love you" was opened by an account representative, even though IT had warned that there was an issue with these emails. It seems there are individuals that will open up these types of emails for any reason. Within the next hour, every image on every computer attached to the server, were destroyed. Part of the code was to also send an email to everyone on the Outlook list for each computer as they were infected. The result was a loss of a day's work related to images and over a week to ensure everything was clean and then the backups installed. This same type of issue has occurred with the installation of malicious IoT devices.

The primary method of avoiding cyberattacks through IoT devices is simply to work with your company's IT department. If a vendor approaches and suggests that they can install the device around your IT department and it provides cyberinformation (sends information) or cyberphysical (can be operated via the internet) capabilities, then be very wary. While it seems inconvenient, IT professionals are the present focus of information on how to deal with cyberattacks by software-related organizations and the government.

Ensure that your company or department has a cybersecurity policy in place. This includes such things as ensuring that: firewalls are not compromised; malware security software is installed and active; and virus protection, including browser protection, is installed and updated regularly; devices that are to be installed and attached to the network are evaluated. Systems that should be excluded from the internet should be installed on separate networks. Finally, training on cybersecurity and its impacts should be performed for all personnel.

Companies and organizations that are particularly vulnerable may also hire cybersecurity IT professionals to monitor and develop strategies to protect the organization. These IT professionals provide a preventive source and help to develop recovery strategies for when cyberattacks are successful.

CONCLUSION

The application of IoT devices is a significant opportunity for the physical asset management industry. The ability to have instant access to information and control over systems through cyberinformation and cyberphysical means is immeasurable.

However, these systems have a significant potential to open an organization up to cyberattacks by cybercriminals. Where these attacks are launched from is becoming more difficult to determine, so the avoidance of the conditions which would make an organization vulnerable is paramount. As put by federal cybersecurity committee members, the growth of IoT and systems is outpacing the ability to regulate and protect against cyberattack.

It becomes equally important that organizations include cybersecurity policy as part of their IoT strategy and educate employees and vendors in these policies. Ensure that companies that describe ways and means to bypass such policies are avoided as even the best companies can become vulnerable as well, opening your organization to their weaknesses. As such, your organization's policy must also include strategies to recover from cyberattack as, statistically, some will get through even the best systems.