FMJ

IFMA™
International Facility Management Association

WWW.IFMA.ORG/FMJ | NOVEMBER/DECEMBER 2016

LEVERAGING LEAN

FOR FM PROCESS IMPROVEMENT

P/44

DON'T MISS

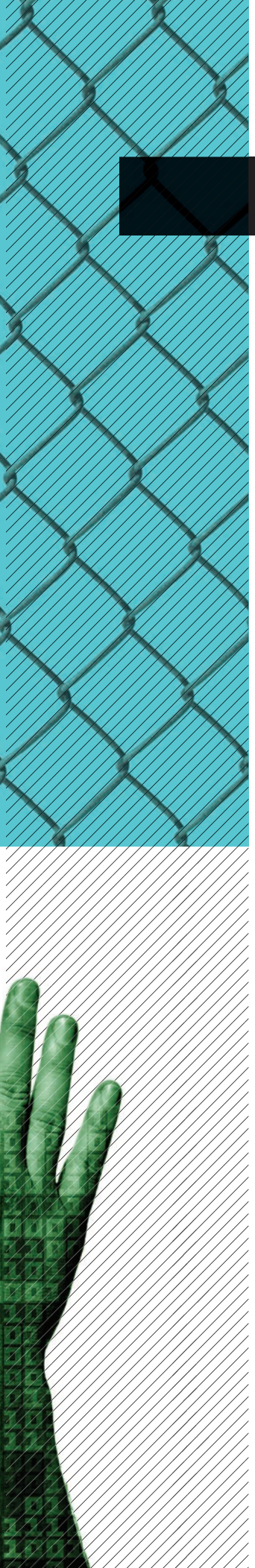
ALIGNING FACILITY GOALS WITH SECURITY EXPERTISE
P39

AN ARGUMENT FOR DATA ANALYSIS
P66

defending your organization against

CYBER INTRUSIONS

This article originally ran in the November/December 2016 issue of FMJ, the official magazine of the International Facility Management Association, and has been reprinted with permission. For more information, visit www.ifma.org/fmj, or visit www.ifma.org/fmj/subscribe to begin receiving FMJ.



BY AL BERMAN AND ANTHONY PIZZITOLA

By now facility managers know the obvious threats to facilities: natural disasters and man-made and technological dangers. Most are prepared for natural and man-made threats, but may feel that the technological is out of our league. While we prepare for what we think will produce the greatest protection, we can be reminded of a quote from Mark Twain – **"What gets us into trouble is not what we don't know. It's what we know for sure that just ain't so."**

And while prevention and preparedness for the dramatic is easy to understand and justify, Twain would tell you it may not be the greatest danger.

The real threat of cyber attacks

Over the last 20 years, cyber intrusion and now terrorism has become the invisible threat that attacks industry, government and individuals every second (and nanosecond) of every day. The number of attacks is incalculable, but one government agency in the United States estimates 10,000 attacks every hour. Facility managers must understand that any disaster can cause them to lose their jobs.

Often the most nuisance disaster is graffiti easily corrected by repainting. Similarly, in 1997 IBM conducted a survey on "who are the hackers" and found that 90 percent were amateurs determined to demonstrate their ability to penetrate systems for the bragging rights. These cyber joyriders were benevolent intruders whose only gain was the satisfaction of proving that they could just do it.

The world today is very different and very expensive — 65 percent of the hackers are business people whose only job is to create financial gain from their efforts. Ten percent are involved in cyber espionage, and the remainder are activists whose goal is to expose what they feel is unethical or illegal activities of government, companies or individuals. Their activities range from disclosure of documents, to interruption of operating sites through denial of service or the destruction of information and communications capabilities.

Cyber-terrorism costs

It is the cyber-terrorists who present the biggest problem and require the greatest effort to contain. The hack for gain proponents come in many forms. The estimate of the financial impact on world economies is difficult to ascertain. In 2000 PricewaterhouseCoopers estimated the financial impact as in excess of US$1.5 trillion. Estimates today range anywhere from US$5-15 trillion.

We have spent a good deal of time looking at the economic model that today's hackers have developed, and if you want to see an efficient business model that has a sophisticated pricing model, the ability to create data warehouses that share information about victims of cyber intrusion, that has a quality control model that would shame some of our best institutions, plus the ability to create efficient joint ventures — then cyber intrusion is the future economic model.

Many of us are aware of the how institutions have simply paid hackers to give them back control of their systems and data. Cyber ransom has become one of the most efficient kidnap and ransom models in the history of civilization. It involves no

physical risk of actually taking possession of a person or asset. No getaway cars, no hideouts, no money drops, no proximity to the victim and almost no chance of being apprehended. It involves simply encrypting the data of an organization or individual so that it is no longer usable. The cyber kidnappers then charge what is a nominal fee (ranging from a few hundred dollars for individuals to less than US$20,000 for organizations). Far less in terms of time and money than it would take for anyone to undo the damage, so it is truly cheaper to pay than to fight.

Those held hostage have ranged from hospitals, to financial institutions, to careless individuals. It is estimated that just one of these cyber-kidnapping organizations netted US$347 million last year. Yes, the typical damage from a hurricane is several billion dollars, but we know it's coming. We are not always prepared for the cyber pirates.

The spread of cyber-crimes

The traditional stolen individual identification information hacking has taken on greater sophistication. It has taken 15 years for the U.S. to actually have chips embedded in their credit cards. The hacking of point of sales machines at Target and Home Depot made headlines around the world because of the magnitude of the intrusion. Tens of millions of individual accounts were stolen and the information sold on the dark web to the highest bidder. Our ability to defend against this has been ineffective and at times showed the futility of trying to react to the relentless and sophisticated world of cyber terrorist innovation.

To understand the sophistication of cyber criminals and their sole goal of financial gain, one has to look no further than the group of hackers known as the FIN4. This group has not stolen identities, has not sold the information to anyone, has not bragged about their conquests or gained notoriety by the magnitude of the information they compromised. They simply wanted to have a trading edge. Their targets were the pharmaceutical companies and more specifically the area involved in research and development.

Their objective was to find out the results of the viability of the new miracle drugs that were in the clinical testing stage. So they hacked pharmaceutical companies and their attorneys, hospitals conducting clinical tests, and even the U.S. Centers for Disease Control and Prevention to obtain inside information so they could gain by buying options on those companies with a high success probability before the information became public. None of the financial gains of the FIN4 are even calculated as part of cyber terrorism.

Cyber-security in your facility

Just as safety is everyone's job in a facility, so is cyber security. How so? Facility departments typically use computerized maintenance management systems for project planning and maintenance routines. Operations are being tied to a computer more and more, and IT is a way of life and to the bank. Attacks can be generated simply by opening a phishing email advertising a free seminar or new product to save time, so check your sources prior to opening. As a solution, companies now have the capability of tagging a suspicious email and sending directly to security personnel for surveillance.

Faced with the daily onslaught of cyber probes and actual cyber attacks we need to provide at least the front lines of prevention. This calls for extreme vigilance and a need to ensure that we are communicating with organizations and

individuals who are as safety minded as we are. This requires that we understand the cyber security environment of our vendors and suppliers. Increasingly, regulations are requiring "due diligence" in dealing with third parties. Make sure your organization has a policy for vendors and suppliers, and be sure to follow it. Be wary of suspicious emails and their origins. Understanding the contents of email headers (a relatively simple process) can help you determine that messages masquerading as legitimate communications actually originated from a suspicious source.

Passwords should never be compromised by open distribution. A complex password is more difficult to break, even when the cyber intruder is using a password breaking app. Establish a policy for everyone to change their passwords routinely. Create a policy that social media is banned while at work, even on cell phones. Control intruder access, and you control your career.

On the subject of cell phones: It is estimated that there are 120 million apps, 10 percent of which have malware intentionally embedded in them. As Android sought to overtake Apple in the creation of apps, the quality control and normal protection were relaxed in order to penetrate the marketplace. Two years ago, Forbes magazine reported that 97 percent of all smartphone malware was found in Android systems. Last year hackers managed to embed malware in the Apple toolkit that is used by developers to create Apple Store apps. Over 4,000 apps were later found to contain the malware which would steal information from smartphone users.

Finally, continue to communicate with your disaster and business continuity professionals. This is a culture that will enhance your knowledge. Participate in tours and help identify small issues that will become larger and more expensive to repair or replace in the future. Remember, cyber security attacks can destroy the security on which you and your department depend. **FMJ**

Al Berman, MBCP, CBLA, is the president and CEO of Disaster Recovery Institute International. An expert on disaster preparedness and recovery, he is an advisor to government and corporations.

Anthony Pizzitola, CFM, MBCP, FBCI is the only IFMA Certified Facility Manager to hold these three significant designations. With experience as a facilities, disaster recovery and quality assurance professional, he is currently a director of business continuity outreach with DRI International.