New World Order:

Organizations and the Threat of Cyber Terrorism

Terri Howard
FEI Behavioral Health

March 2016

fei workforce resilience

New World Order:
Organizations and the Threat of Cyber Terrorism

Cyber-attacks are traumatic experiences impacting employees, customers and the bottom line.

The phenomenon of cyber terrorism and cyber-attacks is one that businesses, if not society in general, continue to underestimate. Since the millennium technology, and the reliance on it, has developed at astonishing speeds—and so has malicious software. For every high demand user experience developer and software engineer, there is someone else using the same skillsets to hack into corporate systems. Sony Entertainment learned this the hard way, as did Las Vegas Sands Corporation, Ashley Madison, Kickstarter, the Internal Revenue Service and the Office of Personnel Management, to name only a few.

Business can be slow to change, but the rate at which the world is progressing is causing such disruption to normal operations that timely, regular evaluations of digital infrastructures and safeguards is required. A cyber-attack does not just mean a blow to the bottom line; it directly impacts the workforce and customers through stolen identities and exploitation of private information. It is a traumatic and fear-inducing experience.

An employee or customer whose data is stolen can spend years enduring the consequences, open to re-victimization if and when cyber terrorists continue to use the information again and again. It is an employer's duty to ensure that every effort is being made to protect its workforce and clientele, and this includes the protection of online identities.

Cyber Attacks on Human Lives

Literature exists downplaying the correlation of terrorism with cyber-attacks. RAND Corporation's Martin Libicki wrote a *Newsweek* article titled "Cyberattacks Are a Nuisance, Not Terrorism," arguing that true terrorism, by definition, is a *physical* threat. [1]

This way of thinking about cyber-attacks invites serious reconsideration, however; the notion that someone's data is immaterial is a misleading one. Reluctance to provide credit card information over the internet in the late 1990s/early 2000s has evolved into in-app purchases over one's smartphone, providing personal information on multiple social media websites, online education and career options, and online banking. As of 2016, the list supporting a digital presence which acts as an extension of an individual's identity is beyond extensive—and that presence is extremely vulnerable to attack.

Who is after this data? News outlets can easily reduce the Sony data breach to a retaliatory North Korean cyber-attack, for example, but the realities of cyber terrorism and its impact are much more complex, as are the people and motives behind the act. Developed with Michael Kaiser of the National Cyber Security Alliance, the following are key types of cyber terrorism being employed today:

- **Cybercriminals** are motivated by money and are typically responsible for hacks such as retail data breaches and phishing attacks. There is high risk to individual customers in terms of compromised personal or financial data and identity theft. An example would be the 2013 hack of Target Corporation, which by extension involved numerous banks.

- **Nation states** engage in cyber terrorism to gain intelligence or sow disruption. The danger here centers on corporate or industry infrastructure—everything from Wall Street to transportation to the electric grid—or on massive data collection, though the ramifications often spill over to individual consumers through city-wide loss of services. The aforementioned attack on Sony by North Korea is an example of the latter.

- **Hacktivists** and hacktivism are more likely after small-scale disruption, embarrassment or justice seeking, rather than personal financial information. The Impact Team's attack on the Ashley Madison website or the work of hacktivist group Anonymous are examples of this type of cyber-attack, and can cause deep emotional pain and privacy violations.

[1] http://www.newsweek.com/cyber-attacks-are-nuisance-not-terrorism-305062

Whatever the means behind the breach, the leaking of personal data results in cyber-crime victims. The effects of a cyber-attack can be traumatic and long lasting for victims, burdening them with emotions as affective as those resulting from physical crime.

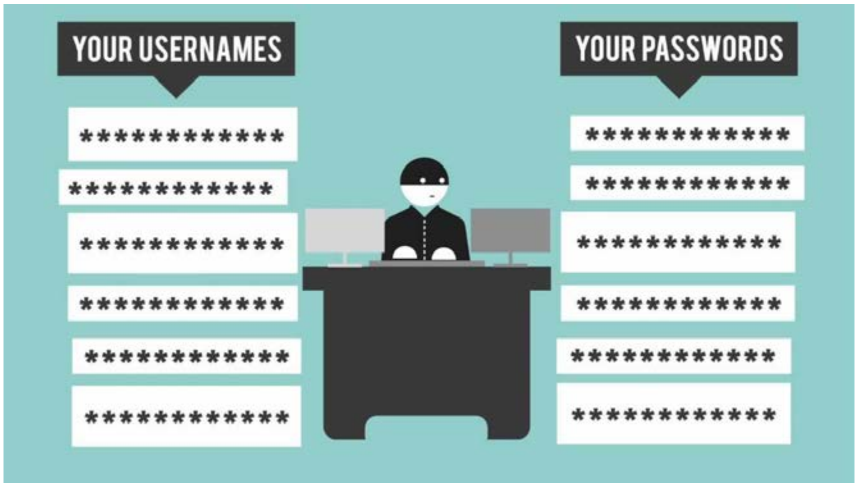
“Am I not taking enough precautions?”

“Do I provide too much information online?”

“How could something like this happen to me?”

The experience can lead to blaming—of self *(“Am I not taking enough precautions?”*; *“Do I provide too much information online?”*) and of others, be they service providers or employers (*“How could something like this happen to me, your client/employee?”*; *“What will you do to protect me and my family from the people who stole our information?”*).

While financial loss is one major outcome of a cyber-attack, breaches also can lead to identity theft. In 2014, more than 12 million U.S. consumers had $16 billion stolen from them due to identity theft. [2] According to Kaiser, all victims of identity theft had some form of their personally identifiable information (PII) used to fraudulently obtain goods, services, jobs, benefits or medical services.



[2] http://www.iii.org/fact-statistic/identity-theft-and-cybercrime

Examples of PII are:

- Name, address, social security number, date of birth, driver's license, etc.
- Medicare or health insurance number
- Bank account or credit card numbers
- Passwords *(including maiden name)*
- Biometric data *(fingerprint, iris scan)*

The effects of compromised PII can be devastating and harmful to victims, including threats like:

- Reduced ability to escape a domestic violence abuser or stalker
- Financial loss
- Denial of employment or housing
- IRS problems
- Time and cost of repairing damage

The average out-of-pocket cost for recovery is $1,870. According to the Bureau of Justice Statistics Special Report, more than three million people experienced issues such as having utilities cut off, being arrested, finding erroneous claims on their health records, having child support garnished for children they never had and being harassed by collection agencies.

Preparing for the Worst: *An Organization's Responsibility*

> "When will *I* be the target of a cyber-attack?"

The question for organizations is no longer "Will I be the target of a cyber-attack?", but rather "When will I be the target of a cyber-attack?" In 2015 alone, 82 percent of surveyed organizations expected to face a cyber-attack. [3] The threat of attack is constant, and businesses must be prepared to protect themselves, their workforces and their clients when the time comes.

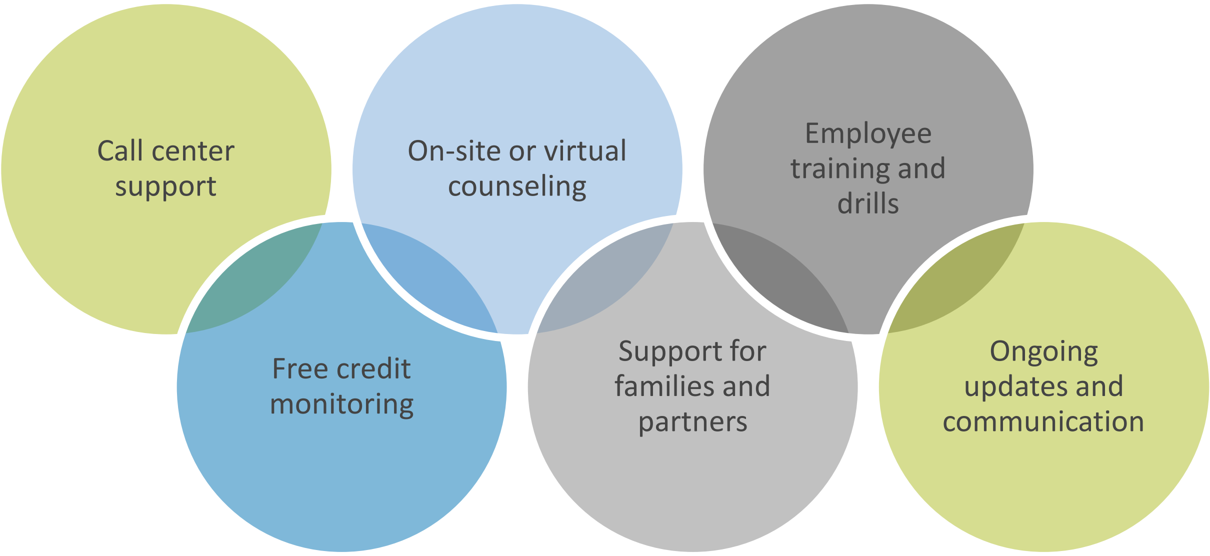
Aside from keeping infrastructure up to date with best practices and security measures to ward off potential attacks, organizations need a detailed response plan to address the impact of such attacks on employees and customers during the days, weeks and months that follow.

[3] http://www.tripwire.com/state-of-security/latest-security-news/80-of-organizations-expect-a-cyber-attack-in-2015-shortage-of-it-pros-threatens-readiness/

Potential challenges can include:

- A reliance on technology, and backlash when technology is made unavailable.
- Communicating relevant information to staff and other stakeholders in a timely manner, with limited or no use of technology.
- Containing information about breaches from leaking to the media, especially if staff and clients have yet to be informed.
- Addressing an influx of questions and concerns from employees—both those who are currently employed and those who have left the organization—about the breach, the state of their information, what is being done in response, etc. This also applies to existing and terminated clientele.
- Handling the volume of inbound inquiries from external stakeholders, media and the public in the wake of such breaches.

To counter these questions and concerns effectively, an organization's response plan should detail how the company will assist its employees and customers in dealing with the attack through elements like:



Call center support

Free credit monitoring

On-site or virtual counseling

Support for families and partners

Employee training and drills

Ongoing updates and communication

Ongoing updates and communication cannot be stressed enough. In a culture reliant on technology for a steady flow of information, separation from a company's network in a time of crisis can be disorienting and chaotic.

Communication protocols that rely on telephonic or face-to-face interactions should be established; this can include an on- or off-site EAP provider, staff counselors, critical incident responders and/or the human resources department. Many organizations do not have the resources internally to support every victim of a cyber-attack, so knowing where support is coming from beforehand is important.

A good plan also outlines a process for quickly assessing the scope of an attack's potential human impact. By formulating policies in advance based on the most likely attack scenarios, companies can stay one step ahead in their preparations.

Like any crisis plan, a cyber-attack response plan is only as good as the training behind it. Employers should routinely conduct drills so their employees know their roles and responsibilities and feel comfortable and competent in responding during an actual attack.

The best order of business for any organization is to offer help to its employees and clients for recovery stemming from cyber-attacks, including:

- Education on and preventive measures against re-victimization.
- Help with contacting credit reporting agencies to place a fraud alert, determine if a credit freeze may be useful and request or review the employee's credit report.
- Training staff on ongoing evaluation of the threat, such as checking credit and bank statements. Some companies go as far as to implement proactive employee and consumer education programs about online safety and security basics.

The FEI Difference

Taking precautions after a cyber-attack must go beyond credit monitoring and internet safety tips. Organizations need a fully realized crisis communications plan that addresses what to do before, during and after a cyber crisis. One that is re-evaluated on a regular basis in order to maintain pace with the ever-evolving world of digital infrastructure.

> *Victims of cybercrime run the gauntlet of anger, guilt, isolation and vulnerability.*

Remember, victims of cybercrime do not just lose a credit card or account passwords; they lose the sense of privacy and control over multiple aspects of their lives—from medical histories to social security numbers and identities—for an unknowable duration. It is not uncommon for victims of cyber-attacks to experience similar responses to other types of trauma, running the gauntlet of anger, guilt, isolation and vulnerability. These emotions can foster behavioral reactions that include difficulty concentrating, insomnia, loss of appetite and absenteeism, while physical reactions range from sweating and aches and pains to heart palpitations.

At FEI Behavioral Health, crisis management experts have developed specialized services to address the human side of emergency response, including cyber-attacks, through the integration of its mental health expertise, critical incident experience, and state-of-the-art call center and information technology. FEI assists organizations with the human side of business recovery, helps manage the crisis effectively to assure business continuity, and provides meaningful support to victims, victim families, and the organization’s employees.

> *FEI’s specialized services address the human side of crisis.*

New World Order:
Organizations and the Threat of Cyber Terrorism

With crisis management and employee resilience becoming increasingly associated with the vulnerability of workplace networks to cyber-attacks, FEI's crisis management experts augment an organization's ability to:

- Develop best practice crisis plans for responding to the needs of employees and their families during and after a breach.
- Communicate continuity plans, operational information and organizational needs.
- Immediately respond to employee and family inquiries.
- Compassionately reach out to employees and families and track needs and services.
- Collect, sort and maintain information through use of FEI's exclusive web-based information system.
- Effectively manage employee and family assistance response efforts.
- Mitigate the effects of trauma post-attack.

> *"FEI's handling of the situation made the partnership a success. If needed again, we would turn to FEI."*

For more than 35 years, FEI has responded to hundreds of customer's critical incidents and has provided crisis support following workplace violence, natural disasters, aviation accidents and acts of terrorism.

Now, with the advent of cyber-attacks on employers and their people, FEI is equipped to utilize its decades of experience to prepare organizations for the worst via support and consultation. Should the worst indeed happen, FEI will be there—providing onsite assistance, EAP resources, and handling both internal and external communications on behalf of the client.

"The biggest benefit of having FEI onboard is that they hit the ground running during a crisis," said an FEI client after a data breach. "FEI's handling of the situation made the partnership a success. Their involvement was ongoing, especially in the early days of the breach."

"If needed again," said the client, "we would turn to FEI for their ability to handle this type of crisis situation."

fei workforce resilience

FEI partners with you to protect and enhance your workforce effectiveness and organizational resiliency. We offer flexible solutions for the full spectrum of your workforce resilience goals, from EAP and wellness to crisis preparedness and management. We leverage our proven resources, compassionate experts and robust network to improve your employees' focus, empower your managers and prepare you to handle the unthinkable crisis, so that you can maintain a healthy, resilient organization.

phone: 800.987.4368
fax: 414.359.1074

Milwaukee, Wisconsin
New York, New York
Atlanta, Georgia

website: www.feinet.com
email: info@feinet.com