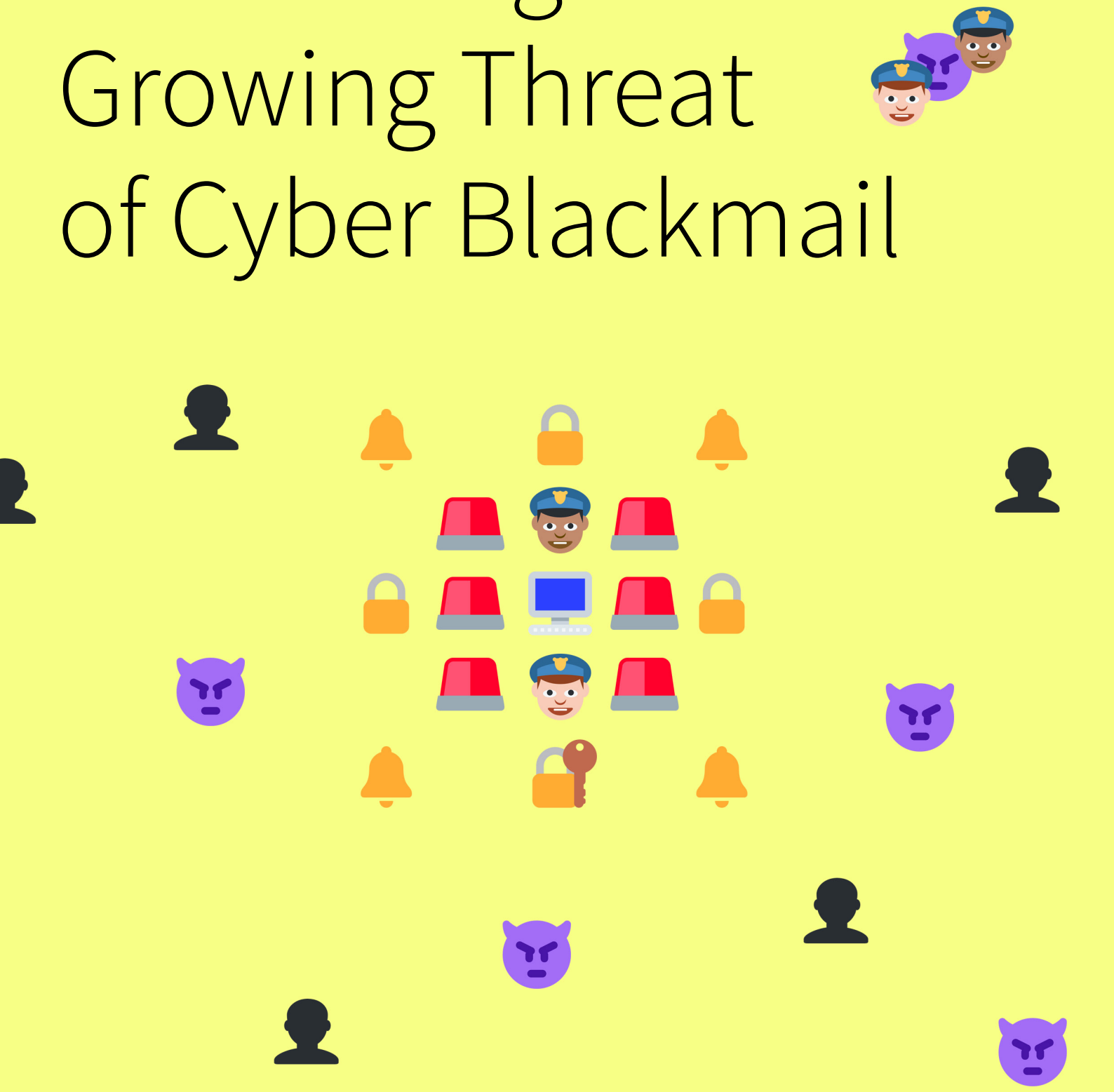
# Countering the Growing Threat of Cyber Blackmail



**Thomas G.A. Brown**
Senior Managing Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting

**Christopher Tarbell**
Managing Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting

FTI CONSULTING™

Extortion and blackmail have been around for centuries. Until recently, criminals who pursued this illegal conduct had to operate in the physical world, limiting the scope and reach of their illicit activities and materially increasing the risk that they would be identified and arrested. Today, thanks to the ubiquitous digitization of our world — especially companies' reliance on computer systems to conduct business — cyber extortionists not only have many more avenues by which to steal sensitive information or hold individuals or companies at ransom but also the means to target a broader array of victims and do so with impunity. With just the click of a mouse, criminals can launch devastating attacks that shut down corporate websites or quietly infiltrate computer networks to steal trade secrets and other valuable information. Information-age extortionists can be thousands of miles away from their victims; proximity is unnecessary in our wired world. Anonymizing technologies such as Tor and virtual currencies like Bitcoin also enable online criminals to conduct their illicit trade with anonymity and without fear of detection.

And just as the Prohibition Era saw bathtub-gin entrepreneurs create mammoth criminal organizations, cyber blackmail has quickly grown from penny-ante, one-off hits to sophisticated operations capable of extorting large sums of money from businesses.

Although much of this activity remains unreported, the risk to enterprises is growing. Computer hackers understand the low-risk/high-reward dynamic of cyber extortion and blackmail and have quietly turned their attention to these lucrative pursuits, holding hostage companies' intellectual property, reputation and even ability to function.

Cyber blackmail presents corporate leadership with the age-old dilemma: to pay or not to pay. The answer is complicated because it's not always clear what you are paying for — will I get back every digital copy of my stolen trade secret, for example, or will the extortionists be satisfied with a single payment? But there are steps companies can take to avoid being placed in this perilous position in the first place and protocols that can help guide organizations once they find themselves there.

## Cyber Blackmail and Extortion: A Growing Threat

The hack of Sony Pictures Entertainment in late 2014 has drawn more attention than any previous cyber extortion plot and could cost the company millions in revenues and reputational damage. According to U.S. law enforcement, the North Korean government was behind the attack, apparently offended by one of Sony's soon-to-be-released films, "The Interview," whose plot was the planned assassination of North Korean Supreme Leader Kim Jong-un. When Sony refused to cave in to the hacker's demands to stop the film's distribution, the hackers not only released data stolen from the company's servers, including other unreleased movies, insider emails and sensitive employee data, but also used destructive malware to cripple many of the systems used by Sony's employees to conduct business.

In an attempt to appease the hackers and stop the bleeding, Sony belatedly took the unprecedented step of canceling the release of "The Interview," taking a significant hit in lost revenues and production costs. While Sony ultimately offered the movie to consumers in a small number of theaters and via video-on-demand, the entire cyber attack still could **cost the company in excess of $100 million**, including costs associated with investigating the attack, rebuilding computer networks, and lawsuits filed in the wake of the hack's public disclosure. (A more targeted attack that shut down Sony's PlayStation network for several weeks in 2011 is reported to have **cost the company $170 million**.)

Beyond quantifiable financial effects, Sony's reputation suffered as its corporate dirty laundry was paraded throughout the media and as President Obama publicly criticized the company's initial decision to cancel the release of "The Interview." Then, in late January, Sony announced that its computers — including its financial and accounting systems — were so compromised by the hack (**which reportedly included the destruction of network hardware**) that it would not be able to report its third-quarter earnings on the February 4 due date, **requesting an extension to March 31**. Sony suggested that the reporting delay would not have a material impact on its financial statements, but the move could not have instilled investor confidence. In early February, the company's co-chairman and head of its

film studio **stepped down**, a move widely reported to be a result of the attack.

The average company may think a lower public profile protects it from such a damaging cyber extortion. But while the Sony hack was unprecedented in its scope and the public interest it generated, the Assistant Director of the Federal Bureau of Investigation's ("FBI") Cyber Division — the FBI's top cyber agent — said it is likely that **90 percent of U.S. corporations — large, midsized and small — are equally vulnerable to such an attack**.

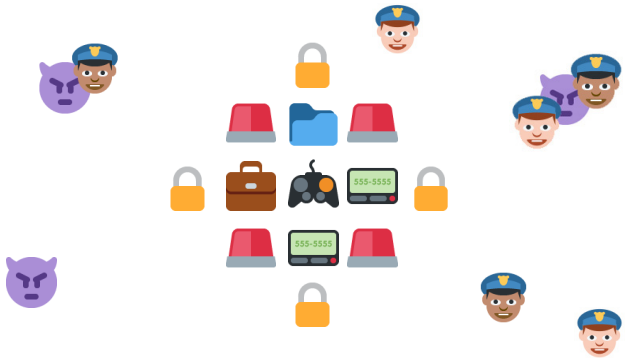
While the Sony Pictures hack has received an inordinate amount of attention, the past 12-24 months, in particular, have been busy for cyber criminals. In June 2014, **a U.S.-led international operation disrupted an Eastern European crime ring** that infected as many as a million computers around the globe with software designed to steal passwords. The gang used the scheme to steal more than $100 million, ranging from $198,000 in an unauthorized wire transfer from an unnamed Pennsylvania materials company to a $750 ransom from a police department in Massachusetts to unlock its investigative files (the files had been rendered inaccessible by **CryptoLocker**, a species of malware that can encrypt data on computers running Microsoft operating systems).

Other recent high-profile cyber crime incidents include:

- A February 2015 data breach at one of the largest health insurers in the United States, Anthem, that potentially exposed the medical information (and the Social Security numbers and home and email addresses) of 80 million customers.

- A point-of-sale hack that resulted in the theft of credit card information from the U.S. restaurant chain P.F. Chang's with **thousands of the stolen cards put up for sale on the so-called "dark web."**

- A breach of security at the Montana Department of Public Health and Human Services in May 2014 that may have **exposed the information of more than a million people.**



- A February 2014 hack of **eBay that reportedly stole the personally identifiable information of 233 million users.**

- **High-profile cyber attacks against Target and The Home Depot** that resulted in the compromise of personally identifiable data for millions of customers.

## The Threatscape: Attacks, Perpetrators and Victims Vary

Would-be cyber blackmailers can initiate their criminal efforts far outside a company's network. One common approach is known as a denial of service ("DoS") attack. Here, thousands of "zombie" computers (secretly controlled by hackers without the knowledge of the computers' owners) are marshaled to launch a simultaneous assault on a target computer resource such as a website, knocking it offline. DoS attacks especially can be damaging to enterprises that rely on user access to their websites, such as e-commerce companies, to conduct business.

Apart from DoS attacks, cyber criminals may seek to break into companies' computer networks. Once inside, hackers can quickly and easily follow any number of vectors to extort money from their victims. Some of the tactics include:

- Encrypting data that exist in business systems, then holding the information hostage for payment.

- Disabling critical business systems.

- Blocking access to corporate sites.

- Redirecting part or all of a corporate website somewhere else by altering DNS (a service that controls website naming and Internet traffic direction) settings, holding the original destination hostage.

- Stealing intellectual property and threatening to sell it to competitors.

- Accessing a computer, downloading unwelcome content (e.g., child pornography) that can't be removed and threatening to call law enforcement unless payment is made.

- Posing as a "gray hat" company (hacking firms that identify weaknesses and fix them for a fee) by finding exploitable weaknesses in corporate networks and threatening to notify the press or competitors unless payment is made.

Individuals also face the risk of so-called sexploitation attacks. In such instances, cyber criminals hijack a user's webcam, microphone or file system to obtain and threaten to release embarrassing photos, videos or messages. In 2010, **the FBI published an alert** for Internet users following the arrest of an California man who hacked into the computers of 200 women, downloaded compromising photos and used them to extort more photos from the victims. Last year, **a man was charged** with threatening to distribute embarrassing pictures of women if they did not provide him with more photos. The most recent high-profile target of such a plot was **Miss Teen USA 2013**, whose webcam was hacked.

Indeed, in May 2014, federal authorities charged an international group of hackers with operating an illegal business that marketed a remote access tool, or "RAT," known as "Blackshades." The Blackshades RAT enabled thousands of hackers in over 100 countries to infect more than half a million computers. After installing Blackshades on a victim's computer, an attacker could access and view documents, photographs and other files; record keystrokes; steal passwords; activate the webcam and microphone; encrypt data; and send ransom notes to the victim.

The Blackshades RAT and similar malware easily can be adapted for corporate espionage. Criminals might commandeer a computer microphone or camera in a boardroom or executive office to film or record confidential meetings. Using that business intelligence, the hackers could blackmail a company, sell its secrets to rivals or manipulate company stock with calibrated releases of privileged information. And cyber extortionists are increasingly targeting the children of intended victims by using information gleaned from social media activities.

Perpetrators of these other forms of cyber extortion range from organized crime rings to unhappy employees. Indeed, attacks are even more insidious when launched from the inside. Law enforcement has engaged **in a number of significant investigations** in recent months involving former or disgruntled company employees. In many of these cases, employees attempted to extort money from employers by threatening to expose privileged information or activate malware. These recent incidents cost victim businesses from $5,000 to $3 million in payoffs.

But, increasingly, the perpetrators of cyber blackmail and extortion are members of organized gangs around the globe.

While breaches of large corporations like Sony Pictures and Anthem make headlines, midsized companies actually may be the most vulnerable. Many smaller organizations fail to invest in redundancies to protect themselves, fearing that even minor changes to day-to-day operations might jeopardize profitability. These companies also lack the personnel and resources required to respond effectively to cyber blackmail attempts. They do, however, have enough capital to attract a cyber extortionist.

## Why Most Companies Dummy Up and Pay Up

The vast majority of cyber blackmail or extortion attempts go unreported. When it comes to insider attacks specifically, three-quarters of the time companies deal with the matter internally and do not disclose the incident to authorities, according to a 2014 **survey of cyber crime by Carnegie Mellon University**.

Many victims of cyber blackmail simply pay a ransom because the consequences of refusing to pay and going public are too damaging to contemplate. Companies don't want to risk their reputation. A major breach often causes customers or business partners to think that inadequate security invited or caused the attack. To many companies, it appears cheaper to pay the ransom than to hire a third party (or devote internal resources) to recover the information, unlock the encrypted data or bring systems back online. Many businesses can't afford to lose revenues if their site goes down anytime — but particularly over the holiday shopping season or, specifically, on Cyber Monday.

But giving in to cyber blackmail demands doesn't always work out as planned. In one high-profile case in 2007, Finnish cell phone company **Nokia not only paid the ransom — leaving millions of euros in a parking lot with the hope that authorities could trace the extortionist — but also botched the delivery**.

The criminal got away with Nokia's cash, and the case remains cold all these years later.

## Alternatives to Capitulation

While it may seem like the quickest and cheapest remedy, giving in to the demands of a cyber extortionist rarely is a good idea. It can be tempting to try to buy yourself out of a problem to keep your business' systems running, retrieve critical data or preserve your reputation. However, capitulating to terrorist-like demands also carries risks. There's never a guarantee that the criminal you're paying off will stay bought, and your customers and business partners will become uneasy should they discover that paying off extortionists is your corporate policy.

In addition, paying a ransom does not address the underlying vulnerability that the criminals exploited in the first place. Only an investigation, in conjunction with law enforcement where appropriate, can reveal the weaknesses that allowed the attack to occur. Such an investigation also can provide a path to remediation that will prevent the specific attack from recurring while also potentially revealing other weaknesses that can be fixed.

There are a number of ways to recover stolen files and data, unlock hijacked systems, and save corporate and individual face without paying or otherwise dealing with manifestly untrustworthy parties.

For instance, **Domino's Pizza** allegedly was attacked in June 2014 by the hacking group Rex Mundi, which claimed it had stolen 650,000 customer records from the company's servers in France and Belgium. Rex Mundi threatened to release those records publicly if Domino's didn't pay a ransom of €30,000. Domino's refused to comply with the demand and instead advised its customers that the stolen data did not contain financial information, only contact details, delivery instructions and passwords. The company instructed customers to change their passwords and began working with authorities and appropriate experts to investigate the incident.

# How to Deal With Cyber Blackmail — Before and After It Occurs

Once a company or individual becomes a victim of cyber extortion, the number of good options dwindles quickly. Rather than react after the fact, corporate leaders need to have a response plan already in place so mitigating the risk of cyber blackmail schemes can be the main focus.

Once it is clear that a company is being extorted by the threat to release stolen information, lock critical data or launch a DoS attack, leaders should:

## Understand the scope of the risks:

- Who are the attackers? Are they hacktivists? Financially motived cyber criminals? State-sponsored actors? Malicious insiders? An effective response depends upon identifying the bad actors.
- How are you or your company being attacked?
- What specific part(s) of your systems are being infiltrated?

## Recognize all potential consequences. Risks come in many forms, including:

- Litigation by injured parties.
- Loss of competitive advantage.
- Reputational damage.
- Cost of response and remediation.
- Regulatory investigations leading to public exposure and possible penalties.

## Have a plan in place. A comprehensive plan should include:

- A list of stakeholders to be informed.
- Predetermined and defined lines of communication that will speed information sharing.
- Appropriately trained and informed leaders empowered to make decisions during an incident (avoiding confusion and a slow response).
- A process for the continuous updating of information technology systems and security policies (at least quarterly) to keep pace with changes in business and technology.

## Take advantage of established relationships with law enforcement (local, state and/or federal) to reduce the chance of a slow, confused response.

Just as important, companies can take a number of steps to lessen the likelihood that they will fall victim to cyber blackmail or extortion:

## Identify all potential internal and external threats by:

- Monitoring social media.
- Staying on top of public forums related to your business.
- Identifying employees who may want to harm your company.

## Audit computer networks to identify and assess vulnerabilities. Questions to ask include:

- Are software patches being applied in a timely fashion?
- Does the network have segmentation so that an attack in one area won't impact others?
- Are there access controls in place for your data?
- Who determines access controls?
- Are network logs collecting sufficient detail to allow for the thorough, informed and efficient investigation of a cyber incident?
- Are network logs maintained for a long enough period of time to allow for proper historical investigation?
- Do you know where all your endpoints are? Are network topology maps up to date? This especially is important because networks are dynamic, with companies continually adding and removing servers and distributing new devices to employees.

# Don't Play the Waiting Game

The cyber blackmail and extortion threatscape will only grow more varied and complex over time. Criminals are continually changing their patterns of attack. While no company can protect itself perfectly, it can make smart investments in due diligence, response plans and sensible security based on rigorous risk assessments of what they stand to lose in the event of such an attack. ■

**Thomas G.A. Brown**
Senior Managing Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting
tom.brown@fticonsulting.com

**Christopher Tarbell**
Managing Director
Global Risk & Investigations Practice
Forensic & Litigation Consulting
FTI Consulting
chris.tarbell@fticonsulting.com

For more information and an online version of this article, visit ftijournal.com.