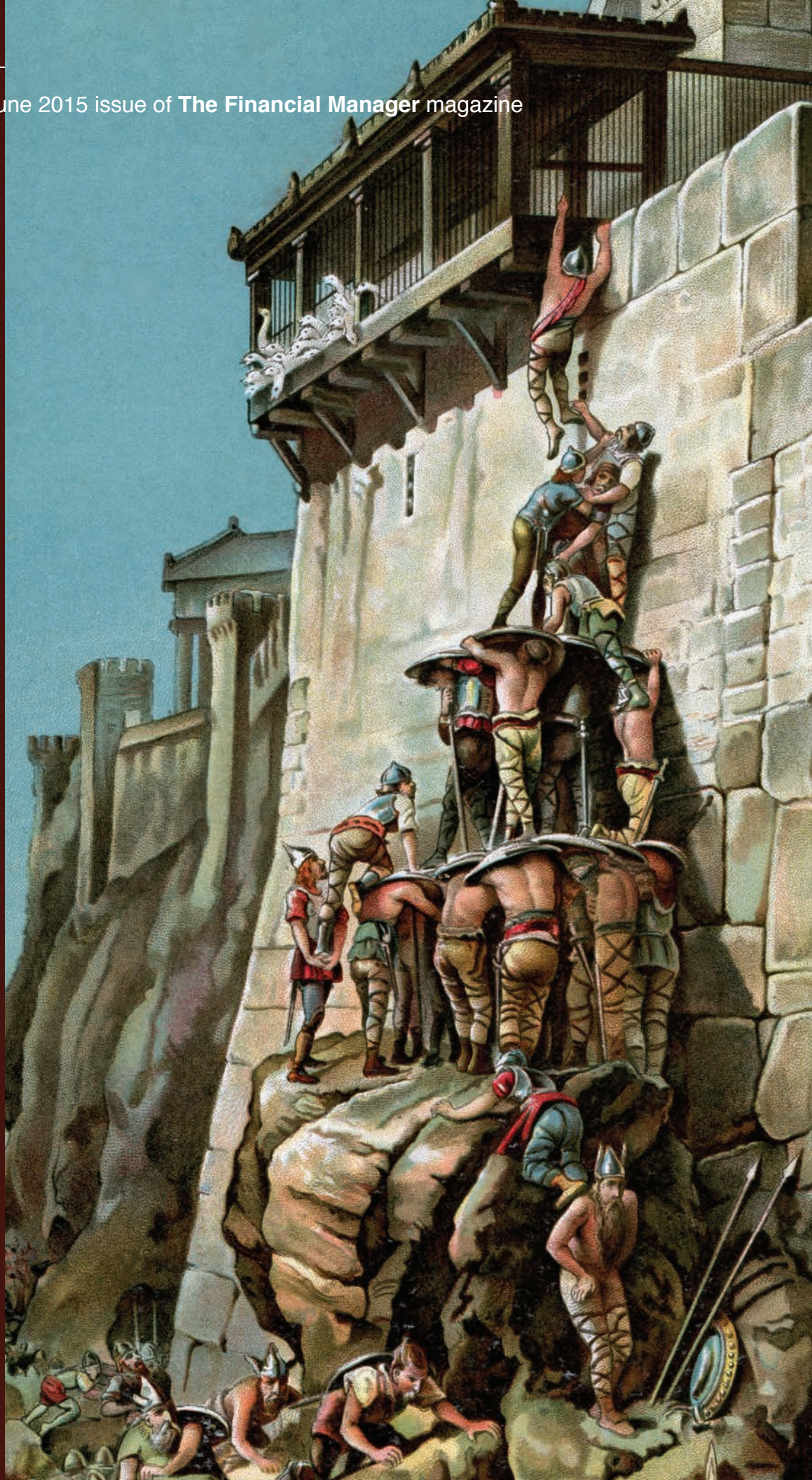
Reprinted from the May/June 2015 issue of **The Financial Manager** magazine

There are a series of measures that should be taken if hackers attack and a company's data "castle" is compromised.



AFTER THE DATA BREACH

By KEN GOLDSTEIN

THE COMPUTER system of a major urban newspaper is hacked, most likely as payback for an article investigating a foreign government. And the passwords of all of the newspaper's employees are compromised.

An employee of a radio network is robbed of his backpack, which contains a mobile device carrying the personal information of thousands of listeners and staff.

A publisher of financial newsletters discovers that hackers have infiltrated computer files containing the contact information, e-mail addresses and passwords of its online subscribers.

It may seem easy to think that those devastating, ripped-from-the-headlines stories will always be nightmares for other companies to face. That could never happen to *your* company, with all its vigilance and an anti-hacker security plan in place, right?

Unfortunately, the answer to that question is "wrong." The odds of a company falling victim to a hacker's attack are increasing exponentially. In a single year, from 2013 to 2014, data breaches across all industries were up an astonishing 48%, according to a study from PricewaterhouseCoopers.

They're also getting more expensive. A Ponemon Institute study estimated the cost of an average data breach in the U.S. at $5.9 million, up from $5.4 million in 2013.

Every business is potentially in the crosshairs. According to a report from Ponemon, the two-year odds of a media company experiencing a data breach involving a minimum of 10,000 records is close to 20%. The report also makes it clear that companies can reduce the cost of a breach by instituting a sound recovery plan.

Here are a series of steps that should be part of that recovery plan – providing a post-breach road map back to normalcy.

CONTACT NETWORK SECURITY AND PRIVACY COUNSEL. Your team's "quarterback" should be an outside law firm with expertise in managing network security and privacy issues. The firm will oversee the mitigation process and the other players involved in it and assist in reporting the event to your cyber insurance carrier.

RETAIN A FORENSIC EXPERT. The role of the forensic expert

is to analyze the suspected breach in order to determine whether, in fact, private and proprietary information has been taken and, if so, to gauge the extent of the damage.

If, for instance, an employee has lost a mobile device containing sensitive information, the forensic expert will determine the specific type of data contained on the device. If a media company has been hacked, forensics will ascertain what information was exposed and how much of it has actually been accessed.

The expert will also give perspective on what the attackers may plan to do with it (sell it, use it for gain, hold it for ransom, or – of particular concern to high-profile media businesses – make it public to embarrass or otherwise damage the company).

BEFORE THE CATASTROPHE

AN INCIDENT response plan (IRP), setting out the company's response to a potential data breach, should be in place before the breach occurs. The plan should answer questions like:

- Who should be contacted if a breach is discovered?
- What information should be passed along?
- What factors should be considered in determining the severity of the breach and a proper response to it?
- What steps need to be taken to restore affected systems?
- How should the incident be documented?

The plan should also include a list of team members, both inside and outside the company, who will be responsible for investigating and mitigating the breach. It could include internal IT specialists, business partners, managers, security personnel and outside forensic experts and counsel.

The network security and privacy counsel should be in charge of hiring the forensic expert so that any reports prepared will be protected by attorney-client privilege.

NOTIFY CUSTOMERS AND/OR EMPLOYEES. Working with forensics, your network security and privacy counsel will determine if the customers and/or employees whose data was exposed need to be notified. If so, the counsel will lay out a plan for notifying them. Forty-seven states (the outliers being Alabama, New Mexico and South Dakota), plus Puerto Rico, Washington, D.C., the Virgin Islands, and certain other international territories, have regulations in place governing whether and how customers should be notified, as well as the time frame for notification.

If a media company has been hacked, forensics will ascertain what information was exposed and how much of it has actually been accessed.

Bear in mind that businesses may be subject to regulatory enforcement proceedings to determine if they've acted responsibly and are in compliance with their own network security and privacy policies. If it's found that they're lacking in those areas, fines may be assessed against them. However, if a company can prove that its data was encrypted, and that the encryption key wasn't compromised, it could be immune from such proceedings.

The notification process can be a challenge for large, multinational media corporations, which may have customers and employees in many different states. Regulations can vary significantly by state – including whether or not individuals can file suit for a breach. This can offer yet another compelling reason for tasking an outside expert with the job.

Partnering with a post-data breach vendor, your outside network security and privacy counsel will determine if customers should be offered services such as monitoring and restoration of identity, credit or healthcare records. They'll also help you determine whether or not a call center should be established, allowing affected individuals to ask questions about the nature of the event, the particular data exposed and the measures being taken to remedy the situation.

MAKE ADDITIONAL NOTIFICATIONS. Many states require that companies notify attorney generals, state consumer protection agencies, credit monitoring agencies and/or law enforcement. The latter may be important if cyber extortion is involved – if, for instance, hackers threaten to reveal, use or sell decrypted private information unless a ransom is paid. Cyber extortion is a growing threat and has already affected several major media companies.

HIRE A PUBLIC RELATIONS FIRM. Data breaches can tarnish a company's image and, depending on the nature of the business, scare off customers, old and new. If, for instance, subscribers to an online newsletter have had their private data exposed as a result of cyber crime or company error such as the loss of a mobile device, they may be less likely to renew subscriptions. And potential customers may look elsewhere for their news, especially if the breach was mishandled or received extensive negative publicity.

A public relations company can be particularly useful in crafting communications with customers who've been impacted by a breach, as well as those whose faith in your company may have been shaken. To control potential damage, you may want to retain a PR firm as soon as the extent of the breach is determined.

REVIEW YOUR VULNERABILITIES. A forensic expert, along with a pre-data breach vendor, can help you determine which processes and systems need fixing. If your employees use mobile devices to conduct business, are their passwords sufficiently strong and is data encrypted? Can the devices be wiped clean remotely in the event of loss or theft? Could a hack have been prevented with intrusion detection software?

In addition to formalizing an incident response plan and using stronger encryption on mobile devices, another best practice can go a long way toward protecting your firm: purchasing cyber insurance. It's worth noting that some insurance companies will refund a percentage of a company's cyber insurance premium if the business takes certain steps to tighten security.

As you consider the potential catastrophes, take the opportunity to look at your company's vulnerabilities. Then strengthen your company's measures to further protect valuable information from future attacks.

Ken Goldstein is a vice president and global cyber security and media liability manager for the Chubb Group of Insurance Companies. He can be reached at goldstek@chubb.com.