By Robert S. Cohen, Esq.

# Hacked! It's Management's Job to Save the Company

## *Three Actions to Protect the Business*

IT'S 3AM…YOUR PHONE RINGS…YOUR HEART RACES…it's your tech guy or CTO…personal credit information records on your lessees and declined lease applicants have been compromised and likely stolen…over 100,000 lessee records! The hackers also gained access to your funding and referral sources! Your customers are exposed and in jeopardy! This is no longer a technology problem…management must save the business!

### What will you do?

You are bombarded with questions. How will I handle 100,000 angry inquiries? What will I say to customers? Will this be reported to the media? Am I obligated to report it to governing agencies? How will this impact my lines of credit? Can this be remedied? How? How much will it cost? Will I be sued? By whom?

This scenario may be avoided if you start to prepare now. Cybersecurity hacks make headlines regularly. Whether it is JP Morgan Chase, Sony, Target or the unexpected email from a friend that just does not look right, we are all under attack. Even when you have a sophisticated security network, it is naïve and irresponsible not to be prepared to protect your company from the horrors of being hacked.

A popular misconception is that cybersecurity preparedness applies only to the technology department. To the contrary, dealing with the fallout of being hacked immediately becomes one of the most important issues facing management. This breach of confidential information can put your company out of business and only management can save it.

This article offers the three-step preemptive strike that will enable management to successfully prepare and minimize the impact of being hacked.

A popular misconception is that cybersecurity preparedness applies only to the technology department.

### Preemptive strike

**ACTION 1:** Create a WISP
**ACTION 2:** Hire an attorney experienced in cybersecurity
**ACTION 3:** Buy "proper" cybersecurity insurance

### Action 1: Create a WISP

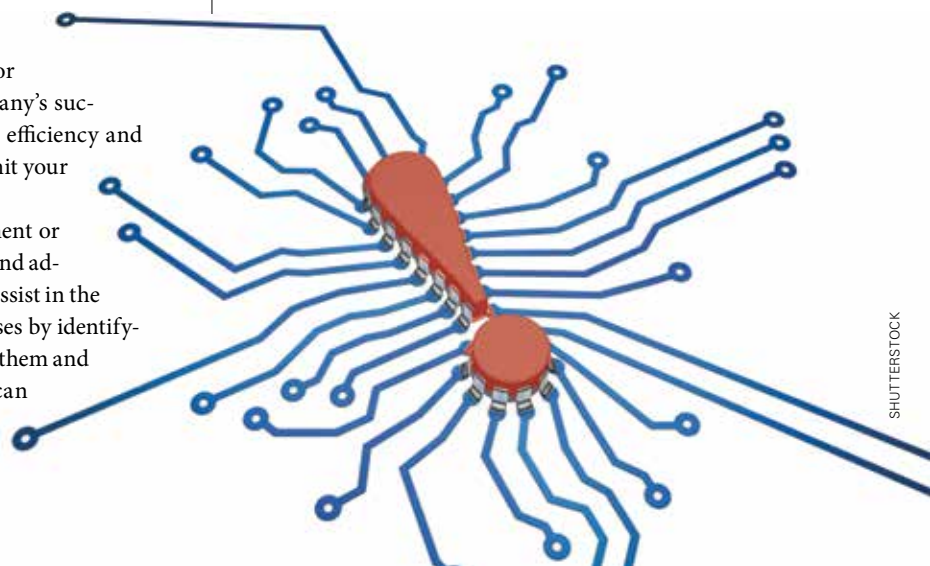
A written information security plan or "WISP" is directly linked to the company's success of recovery. It creates your speed, efficiency and effectiveness to respond. It also may limit your liability.

A WISP is a comprehensive document or handbook that will allow you to frame and address most cybersecurity issues. It will assist in the protection of your network and databases by identifying vulnerable assets, who has access to them and how the security surrounding them can be improved. A well-drafted WISP will also establish procedures and protocols for detecting anomalies in your network and potential breaches (TJ Maxx reported that it took approximately 14 months to discover that they were hacked). A WISP also creates a response plan to a cybersecurity breach identifying the responsibilities of management and vendors that may include companies that provide data security, public relations and insurance. Retention of competent counsel experienced in cybersecurity issues is also critical as your attorney will provide guidance on regulatory matters, notification requirements and professionally draft your WISP. At minimum, your WISP will be a checklist of what to do both before and during a crisis.

A WISP is now mandated or strongly recommended for most companies in the equipment leasing and finance industry pursuant to the Federal Gramm-Leach-Bliley Act, the regulations of the Office of Comptroller of Currency and/or other governing agencies.

### Action 2: Hire an attorney experienced in cybersecurity

The smoking gun…If your company hires outside vendors to perform technology and other tasks, you are vulnerable. For example, using an outside computer security consultant will provide your company with a series of reports detailing your network and highlighting areas for improvement. Most companies will not address all of these recommendations. Subsequently, if your company is sued because of a cyber breach, there is now a report in your file identifying prob-



SHUTTERSTOCK

lems that your company failed to remedy. That report will be a key piece of evidence in the litigation and no doubt used as the 'smoking gun' to demonstrate a lack of responsible actions on the part of your company. This may be avoided if outside vendors are hired through and by your cyber-lawyer who may protect these reports as confidential via attorney client privilege. This simple and small procedural change can have a massive impact on your company's exposure to damages from cyber attacks.

## Action 3: Buy "proper" cybersecurity insurance

Insurance is critical to cybersecurity preparedness. A large portion of costs associated with a cybersecurity breach involve first party costs. Those costs may include: the expenses associated with notifying the affected persons, setting up call centers to address concerns, buying identity theft monitoring, legal fees and more. Many of these costs, including third party damages, may be covered by a smart cybersecurity insurance policy. However, those policies can differ dramatically and therefore should be reviewed with your insurance agent and your legal counsel to determine smart coverage. For example, a typical cybersecurity policy will reimburse the company for damages related to the inadvertent disclosure of certain confidential information or personally identifiable information ("PII"). However, the definition of PII differs dramatically from one policy to another. Your goal is to obtain a policy that defines PII broadly and your legal counsel is best prepared to confirm this for your corporate protection. Cyber insurance is a prudent and very important aspect of your cybersecurity preparations.

## Conclusion

Cybersecurity preparedness requires planning and action. It is a new ongoing process that will continue to evolve. It cannot be ignored. These three actions are an essential and excellent start that will materially improve your company's ability to address, pay for and recover from a cybersecurity breach. The collection of confidential financial information is an integral part of the equipment leasing and finance industry. A company's failure to have sufficient safeguards in place to defend against the unauthorized disclosure of that information is placing the company's business at material risk. This three-prong preemptive strike may save your company. Prepare now and sleep easy.

When the 3am call wakes you with news of a cybersecurity breach, now you are empowered to protect your company. ■

**Robert S. Cohen,** a Partner at the law firm of Moritt Hock & Hamroff LLP located in Long Island and New York City, has over 30 years of experience providing legal services to the equipment leasing & finance industry. He is also a current member of the ELFA Legal Committee.