PALEY ROTHMAN
ATTORNEYS AT LAW

Trick or Treat: Cybersecurity Threats at Your Door

By Ryan Spiegel

Perhaps it's no coincidence that *Cybersecurity Awareness Month* falls in October, the same month as Halloween. Malicious programs can come knocking at the door of your company's digital firewall, dressed in costume as a harmless email attachment or website link. If you open the door expecting a *treat*, you could end up with a costly and damaging *trick*. So it's the perfect time to take note of the cybersecurity risks that your business may face.

This year marks the 10th anniversary of *Cybersecurity Awareness Month*, and there has been a lot of cyber-related news making headlines lately. Adobe, the ubiquitous provider of PDF software, just suffered from a major hacking that compromised an estimated 38 million passwords as well as the source code for its popular Photoshop software. And although it wasn't a cybersecurity event in the traditional sense, the glitches and crashes engulfing the launch of the Healthcare.gov website underscored the vulnerabilities of major web-based systems that handle huge volumes of highly sensitive data.

In compliance with President Obama's Executive Order in February, the National Institute of Standards and Technology (NIST) just released its Preliminary Cybersecurity Framework for public comment. The Framework seeks to establish voluntary minimum standards for protecting critical infrastructure, and the President convened industry leaders at the White House to solicit their input and highlight the rollout of the NIST Framework. Yet as Tom Ridge, former U.S. Secretary of Homeland Security, recently told a crowd at the Montgomery County Business Hall of Fame, voluntary minimum standards just aren't enough. He observed that if your business is exposed to cybersecurity risks, it's not just a *tech* problem to delegate to your IT staff, it's a *business* problem that requires the attention of top management.

Cybersecurity attacks can reduce revenue, steal intellectual property, harm reputations, and cripple all sorts of business operations. And if you think this is a problem only for defense contractors or large companies, think again. Hackers are increasingly targeting smaller businesses that may be more vulnerable because they lack the resources to implement a comprehensive cybersecurity program. When those smaller businesses team up with larger companies or interact with customers, they can inadvertently pass along intrusive malware to others if their systems are infected.

Because the defense industry has increased its focus on cybersecurity, hackers are continuing to target other industries that are not as well-prepared, including finance, energy, construction, and even retail. When you think about all the information from these industries that is now digital – controls for electric utilities, brokerage accounts and credit card information, blueprints for bridges and tunnels – the non-defense arena is a target-rich environment that hasn't invested as much in protecting its systems. Sondra Barbour, Executive Vice President of Information Systems & Global Solutions at Lockheed Martin, told an audience at the Tech Council of Maryland this month that hackers are even reusing methods considered *outdated* by the defense industry to attack systems in other industries that haven't taken steps to protect against these older tactics.

To make matters worse, a cottage industry of so-called "Zero Day" hackers has been created, in which they identify vulnerabilities in a system and then, rather than using the information to access the system themselves, sell it to a third party that wants to access your system. That raises an interesting question: *What sort of legal liability does this digital intermediary have when the actual access or theft is performed by someone else?*

At Lockheed Martin's global cybersecurity headquarters in Gaithersburg, just up the road from NIST, the company has been developing innovative processes for protecting their systems. Perhaps more importantly, it also is educating and training employees to recognize and avoid cybersecurity threats. Lockheed's "Cyber Kill Chain" approach is designed to identify and stop cyber attacks. As Barbour explained, the company uses a sort of "Internal Affairs" method for testing employees' reactions to fake threats that it plants in the workplace, such as vague emails from unknown senders or suspicious USB

thumb drives.

Both Ridge and Barbour noted that the biggest threat to cybersecurity is not foreign nations or outside hackers, but rather a company's own employees. A current employee who inadvertently lets a virus in the door, or a disgruntled former employee who still has access to your system, is actually more likely to damage your business. Policies and procedures to educate your employees and regularly confirm their compliance with security measures can go a long way. Yet merely checking off the boxes on a list of basic steps that your business has taken is not going to suffice, according to Barbour, particularly since the nature of the threat - and the way in which it presents itself - is constantly changing. She contends that many businesses, especially those outside the defense industry, are not paying enough attention to this issue or are fooling themselves into believing that they are adequately protected or are not targets.

Cybersecurity is not only a business and technology issue; it raises a host of legal questions. Barbour relayed business concerns about potential liability arising from the NIST Framework. The Government often considers a bidder's past performance when deciding whether to award a contract. Would a government contractor be disinclined to come forward and notify the Government of a cybersecurity breach if that disclosure lessened its chances to win a future award? Don't we want to *encourage* contractors to make the Government aware of any such attacks and to have them share that information with industry partners, without fear of being penalized? What sorts of new contractual or regulatory requirements might the Government impose on a contractor? What requirements could a contractor impose on the Government? Should the Government indemnify a contractor if that contractor's data is compromised while in the Government's possession?

There is no end to the questions that arise from the myriad of scenarios that could play out. Outside of the government contracting realm, could consumers or shareholders bring lawsuits against a company that does not implement the voluntary minimum standards of the NIST Framework and then gets hacked? How much cybersecurity protection is considered reasonable, and when do the costs outweigh the benefits such that a business won't be held accountable for compromised sensitive data or other damage caused by a hack that could have been prevented?

Could an employee sue an employer for imposing a cybersecurity policy that places too many restrictions on the employee's use of technology, or for taking disciplinary action against an employee who claims he was the victim of entrapment by an overzealous corporate program to test employees' reactions to suspicious emails and thumb drives?

The bottom line is that cybersecurity is too important to be shrugged off. Paley Rothman's Government Contracts, Employment Law, and Science & Technology practice groups can help your business identify the resources and guidance needed to start tackling these complex issues in a meaningful way, because the questions raised by the very real and rapidly evolving threats to cybersecurity infrastructure are downright *spooky*. Happy Halloween.

