ROCHESTER BUSINESS JOURNAL
Part of the BRIDGETOWER MEDIA network
OCTOBER 18, 2024

A brave new world: Responding to a cyber incident

ANNA MERCADO CLARK AND MITCH P. SNYDER

It is Monday morning and you arrive at work eager to tackle the day's challenges. You take a sip of your coffee, settle in at your workspace and power up your computer. Suddenly a menacing message flashes across your computer screen. The message demands a ransom payment and threatens to release sensitive customer data if you refuse. You suddenly realize the unthinkable has happened — your business has fallen victim to a cyberattack. How did this happen? What do you do now? Who should you call?

Unfortunately, situations like this are increasingly common for businesses worldwide and impact businesses of all industries and sizes. Although companies aim to prevent these cyber incidents, there is no such thing as infallible security. If your business falls victim to a cyber incident, your preparedness and how you respond will largely determine its impact.

Having a thought-out and tested cyber incident response plan plays a key role in mitigating potential losses that these incidents wreak on businesses, as well as impact on businesses' reputations.

DEVELOP A RESPONSE PLAN

Planning is essential to implementing an effective and comprehensive response to a cyber incident. So it is important to have a cyber incident response plan and a business continuity plan to guide your team. These plans should be periodically reviewed and/or tested, tailored to your business, and relevant personnel should be appropriately trained.

Consider the following for an effective incident response plan:

- Preparation
- Detection and analysis
- Containment, eradication and recovery
- Post-incident response

Having a plan in place will guide your team when the pressures of the cyber incident are at their worst, which increases the likelihood of an effective and efficient response.

A business continuity plan outlines restoration of operations during unexpected disruption, such as due to a natural disaster, cyber attack, or even a pandemic. The plan, among other things, identifies the essential functions of the business, adopts preventive measures to reduce operational disruptions, prioritizes restoration of day-to-day business operations, and identifies redundancies or alternative work flows or resources. Business continuity planning helps your team streamline your re-

covery efforts in the event of data or system disruption and restoration of operations.

Ultimately, whatever size your business may be, you should have both these plans in place to guide your team in responding to an unexpected crisis, like a cyber incident. If you do not have such plans developed, consider speaking with experienced cybersecurity counsel to create plans tailored to your business's unique needs.

TRAIN YOUR TEAM

Not only should plans be in place, but company personnel should be trained on how to implement those plans effectively. Training will familiarize your team with your policies and procedures so they can effectively implement them when a crisis arises.

Also, review these plans periodically, and update them as needed. One way to train your team is through tabletop exercises, which simulate cyberattacks or other crises. The team walks through scenarios derived from the current threat landscape and is trained on what the policies require as well as the practical challenges that it could face.

RETAIN EXPERIENCED CYBERSECURITY AND DATA PRIVACY COUNSEL

Because of the ever-evolving threat landscape, the need for legal counsel with practical and technical expertise addressing cyber incidents is essential. Experienced cybersecurity and data privacy counsel can guide you through all stages of responding to a data incident.

Counsel can help you develop a plan and train personnel so your team is prepared before an incident even occurs. When an incident does arise, counsel should be a core part of your response team and could help you investigate and contain the incident. Once the incident is resolved, counsel can advise you on any legal obligations arising from the incident and help you take steps to mitigate any risk. Because experienced legal counsel is a key part of any incident response, consider retaining counsel to advise you on navigating the complex legal landscape around cyber incidents.

RETAIN A FORENSIC INVESTIGATOR

As part of responding to a data incident, it is essential to determine what happened. To do this, you should consider retaining a forensic investigator. Cyber incidents are extremely complex and require a highly technical investigation.

Avoid conducting your own investigation or drawing your own conclusions. Instead, it's best to rely on subject matter experts to evaluate the situation and provide the benefit of their expertise.

Further, forensic investigators should be engaged through counsel under the principles outlined in *United States v. Kovel*, via a Kovel letter, which protects the confidentiality of the work undertaken at counsel's direction (i.e., the investigation of your cyber incident and its conclusions). This will allow you to maintain as much control as possible over the confidentiality of your investigation.

KEEP CALM AND CARRY ON

Most importantly, remain calm and do not panic. The bad actors who carry out cyberattacks want you to act out of fear — do not give them what they want. If you have taken the steps outlined above, you will be prepared to implement your plans and have experienced cybersecurity and data privacy counsel watching your back.

Anna Mercado Clark, CIPP/E, CIPP/US, CIPM, FIP, Partner at Phillips Lytle LLP and Leader of the firm's Data Privacy and Cybersecurity and e-Discovery Practice Teams, can be reached at aclark@phillipslytle.com or (212) 508-0466.

Mitch P. Snyder is an attorney at Phillips Lytle LLP and member of the firm's Data Privacy and Cybersecurity and e-Discovery Practice Teams. He can be reached at msnyder@phillipslytle.com or (716) 847-8322.