Published on *The National Law Review* https://natlawreview.com

# Upside Down: Privacy and Data Security LARP

Article By:

Angela P. Doughty

The webinar, one in a series for Ward and Smith's In-House Counsel Virtual Seminar, discussed how to prepare for a security breach, how to preserve evidence, and whether or not to pay a ransom to retrieve vital information.

The session — Upside Down:  Privacy and Data Security LARP — used the firm's signature live-action role-playing (LARPing) technique to guide participants through updates pertaining to data security, illuminated through a hypothetical cyber-attack.

The panel discussion featured insights from Chris Hope, senior director of IT and security at One Source Communications, and Bridget Welborn, who leverages her experience as an attorney specializing in data protection and technology in her role as senior vice president of privacy and records management at First Citizens Bank.

To shed light on how business leaders should prepare for and respond to a cyber incident, session leaders walked participants through a hypothetical scenario involving an attack on a closely held logistics company with a national presence. In this situation, an unknown third party:

- Hacked the company's official Facebook page and posted the names, addresses, and truncated social security numbers of every employee
- Accessed the CEO's email account and sent official-looking spoof emails to all the employees about the information posted on Facebook

"The first step I would recommend starts before any potential incident ever occurs," advised Welborn, "and that is planning." This would include setting up an Incident Response Team (IRT) comprised of key internal stakeholders from the company.

Figuring out who to call first in the event of an incident and getting the right people on the IRT is essential, explained Welborn. For internal stakeholders, Welborn suggested including:

- In-house counsel
- Chief Technology Officer and/or IT professional

- Human Resources
- Outside Counsel

A few other topics to consider as an aspect of pre-planning include finding a forensics firm specializing in data security. “A little bit of pre-planning goes a long way when this type of situation occurs,” noted Welborn.

## Containment and Evidence Preservation

“The number one thing to do on the IT side of things is to make sure it can't get worse,” said Hope. This involves making sure the threat actor no longer has any sort of access. To achieve that goal, a business should change the credentials for compromised accounts and consider shutting down systems, including servers or workstations.

Finding where access has been gained so the problem can be isolated and contained is critical to ensuring things don't worsen. Hope further explained that "What we don't want to do is delete or remove anything from systems because what we can end up doing is compromising the evidence that's available for the investigative team to analyze and understand exactly what happened."

Once the evidence is gone, it can never be retrieved. There is only one opportunity to preserve the data. It is also imperative to know who to call for investigation and remediation. Similar to Welborn, Hope's advice for company leaders is to be proactive and identify all of the parties that need to be involved before an incident occurs.

“It can be really painful to figure these things out on the fly,” Hope says, “so a little bit of legwork goes a long way toward making these incidents manageable.”

## IRT Roles and Responsibilities

When assembling an IRT, it is vital to have decision-makers at the table. Getting everyone together to talk about steps and decisions is a waste of time if someone has to call a time out to find the appropriate party to ask for permission.

"Time is really important once you discover that something has occurred," noted Welborn. "It's also good to have some idea about worst-case scenarios."

Welborn pointed out that, if a situation occurs that requires a notification, a number of questions will arise as a result, including:

1. What type of notification needs to be sent?
2. How are we going to reach out to our employees or customers?
3. Is it appropriate to send a company-wide email if an internal email account has been hacked?

The next scene in this hypothetical cyber incident involves the IT director hiring a forensics company to ascertain as much information as possible. After the forensics report comes back, it confirms that

the email came from the CEO's account, the Facebook post was made 30 minutes later, and both actions originated from the same IP address.

Worse, the forensics report shows that the bad actor:

- Accessed the CEOs login credentials, which granted them unrestricted access to all the company's systems
- Viewed and forwarded a specific email between the CEO and the HR director containing sensitive employee information, including full social security numbers
- Removed that email and the CEO's login credentials from the system completely

## Forensics Reports

A common misconception about forensics reports relates to turn-around time. Instead of minutes or hours, these reports are typically returned in days or weeks. In most cases, there is simply a lot of information to sift through. However, forensics teams are set up to provide clients with consistent updates, sometimes multiple times per day in the early stages of an investigation.

"These updates are not going to be a complete picture," Hope explains, "but there will be enough information to start the decision-making process."

Most reports will include information about who was involved, what happened, and how it occurred. What these reports are not supposed to include is information about legal conclusions.

While waiting for the forensics report, the IRT should begin drafting communications centered on what to tell employees or customers. Doing so can help to prevent reputation damage and ensure that employees have as little anxiety as possible about what happened, noted Welborn.

## Action Items

Oftentimes, a forensics report will shed light on any items that need to be addressed in regards to an organization's privacy practices. "This would be an opportunity, after making it through the investigation and any potential responses that are required, to take a look at your practices," said Welborn.

To prevent another incident, businesses should consider the following:

- Access controls - Lockdown information and data, such that employees only have access to what they need to do their job
- Email practices - Do not share sensitive data in email; instead, direct the user to a secured space

"Aligning people's access to their actual job responsibilities and needs is free," comments Hope. "There is no technology cost, it is just a little bit of time and effort." Taking it a step further, there are a few other measures businesses should consider:

- Encrypted email - Relatively inexpensive and easy to implement
- Two-factor authentication - Especially vital for business-critical information

In this hypothetical scenario involving a company with 200 people, using a two-factor authentication system would cost around $20,000 to $40,000 per year. “When you compare that to the cost of a cybersecurity incident, which averaged around $4.62 million in 2021, that $20,000 to $40,000 is pretty appealing at that point,” added Hope.

## Ransoms: To Pay or Not to Pay?

Publishing truncated information is often just a starting point for many bad actors. In many cases, these cyber-criminals will come back later, threatening to publish all of the stolen data unless the company pays a ransom. Other times, the individual will offer a key to unencrypt stolen information in exchange for compensation.

“The last numbers from North Carolina were published in 2019, showing there were 1,200 data loss incidents,” Hope said. The numbers show incidents that were reported to the State Bureau of Investigation; however, many businesses do not report these incidents to law enforcement.

Around 50 percent of companies will end up paying the ransom. Out of that 50 percent, only around 29 percent ultimately receive what they were promised. “This is a really bad return on investment for what typically represents hundreds of thousands of dollars in cash,” Hope explained.

Additionally, paying the ransom encourages the behavior, inspiring bad actors to return to the well. The incident of repeat attacks is shockingly high, so even if a cyber-insurance provider recommends paying up, organizations should allocate the cash toward prevention by applying increased security measures, or for remediation, by providing affected individuals with credit monitoring services.



National Law Review, Volume XII, Number 12