LEWIS ROCA

RESPOND TO YOUR FUTURE DATA BREACH TODAY

By Patrick McCormick, CIPP/US on 10/26/2022
Posted in Cybersecurity and Data Protection

There is a saying that is often attributed to a Chinese proverb (though its origins are actually unknown) that the best time to plant a tree is 20 years ago, and the second-best time is today.

Similarly, the best time to respond to a ransomware attack was yesterday, but the second-best time to start responding is today.

Study[1] after study[2] after study[3] after study[4] over the past year has confirmed that having a plan in place in the event of a data breach and ransomware attack can save you and your company millions. Every employer has a fire evacuation plan and drills they run, and this is no different.

In the unfortunate event of a data breach, you are going to want to know a lot of critical information very quickly. The good news is that you can gather a lot of that information today:

1. Who in your organization is responsible for each aspect of the response, and do you have their personal contact information?
2. Do you have cyberinsurance coverage and, if so, what is the contact information?
3. Who is your data breach response attorney, and what is their contact information?
4. What is the phone number for your local FBI office? In Arizona, it's (623) 466-1999.
5. What data do you have, and where is it stored?
6. Where is your backup, and when is the last time you checked to make sure it worked?
7. Are you in a specially-regulated industry that imposes a short deadline for providing notice of data breach incidents and ransomware payments, such as health care, health tracking, banking/finance, student data processing, or defense contracting?

Having these answers on hand will save you precious time and money if your system is compromised. Knowing what data you have and where it is stored will allow you to quickly assess what might be compromised and how to best limit further access to your system.

This will also free you up to think more critically about whether to pay the ransom, as there are some questions you likely will not be able to answer until you face a ransom demand:

1. How real is this demand (have the threat actors really exfiltrated your data, or did they gain just enough access to splash a scary demand on your screen)?
2. Is the attacker a sanctioned entity?
3. Will your policy cover the payment?
4. What is the cost of interruption vs. the cost of payment?
5. How likely are you to be a repeat target?
6. Does the FBI have a decryptor key already?

Finally, keep a running list of all your agreements (vendor/supplier contracts, client contracts, etc.) that require notification in the event of a breach. Some of your agreements may require notification within 24-48 hours and may require notification of *any* data breach incident, *not* just an incident involving that party's data.

For more information about developing a data breach response plan and continued awareness concerning cybersecurity threats, contact Patrick Emerson McCormick at pmccormick@lewisroca.com or another member of Lewis Roca's Data Protection and Cybersecurity Team.

---

[1] https://www.verizon.com/business/resources/reports/dbir/
[2] https://www.ibm.com/reports/data-breach
[3] https://www.blackberry.com/us/en/forms/enterprise/report-bb-2022-threat-report-aem
[4] https://www.accenture.com/_acnmedia/PDF-165/Accenture-State-Of-Cybersecurity-2021.pdf

Tags: Data Protection and Cybersecurity