Incident Response

CASE STUDY

Company Overview

A medium-sized credit union headquartered in the Northeast climbed out of the financial recession with ambitions to grow the institution through a series of mergers and acquisitions. During the credit union's annual meeting, the consensus of 500 full-time employees was that the fear of a second recession had passed and securing member information was top-of-mind and forefront in most conversations. Much of this can be credited to the news coverage of large-scale cyberattacks that have resulted in billion dollar losses to institutions very similar to their own.

The CEO admitted that the institution didn't do enough with cybersecurity at the moment and also recognized that it was because they didn't understand it. The CEO also referenced the recent NCUA letter that intended to assist credit unions to prepare for their 2015 NCUA examinations. The letter clearly stated that the association would focus on cybersecurity and that examiners will focus on proactive measures credit unions take to protect their data and members as well as evaluating the credit union's capacity to recover and resume operations in the event a security breach does occur.

Situation Overview

To address this problem and take control of the credit union's cybersecurity narrative, the CEO met with the IT team and mutually agreed that they didn't haev the in-house expertise to produce an Incident Response Plan. They decided that a long and overdue visit to a financial services Cybersecurity Summit was in order. Budgets had been cut in recent years, and this would help bring them up-to-speed. The Cybersecurity Summit would allow an open forum for credit unions to discuss recent cyber breaches, incident response plans, and how to best manage their cybersecurity budgets.

The team's agenda for the summit was simple: educate themselves, find out what their peers were doing, and then identify the right path forward for the institution. Muchy to the surprise of the team, nearly all of the attendees were there for the same reason, which is to say they were trying to figure out the best way to approach incident response planning as well. There were very few institutions that already had an incident response program in place, and the few that did provided the team with great insight into lessons learned from their selection process for an incident response solution and partner.

The universal message and takeaway from the summit was: Don't wait to get started, don't box yourself into a poor solution that doesn't fit, and don't overspend. The CEO and IT team walked away comfortable with this approach amd agreed that they needed a solution that was fast, flexible, and affordable.

Solution Requirements

Fast, flexible, and affordable was what the team felt was right all along, and the Cybersecurity Summit was the gut check that gave them the confidence to move forward. Several key requirements surfaced during the summit with regard to an incident response solution, each of which mapped to the "Fast, Flexible, and Affordable" motto.

- Rapid deployment to easily address compliance mandates (Fast)
- Ease of deployment and use (Fast, Flexible)
- Low total cost of ownership and low installation cost (Affordable)
- Should automatically update and adjust as the Incident Response Plan changes (Flexible)
- Should offer interoperability with other IT Governance, Risk, and Compliance (IT GRC) functions (Fast, Flexible)
- Designed, supported, and maintained by a company who has real-world expertise in cyber breaches (Fast, Flexible, Affordable)

Incident Response

CASE STUDY

Solution Options

The credit union organized a solution review team they called a Cyber Joint Task Force, or "Cyber JTF" for short. The Cyber JTF consisted of a team represented by multiple business units, not just the IT team. (This was one of the lessons learned at the Cybersecurity Summit - incident response affects everyone, not just IT.)

The institution also realized that there were broader needs related to cybersecurity, and they should look to a solution that would allow them to grow into an on-going information security program. The one solution that met and actually exceeded their criteria for incident response was TraceSecurity's cloud-based IT GRC Platform, TraceCSO.

TraceCSO Solution - Advantages/Results

The team favored TraceCSO's cloud-based incident response capabilities, first because of its price, which was priced 30% less than the products the other vendors were pitching. But there were other deciding factors that had much more to do with performance and other strategic issues; specifically:

- Speed of deployment: Their TraceCSO account could be active within hours of signing a contract.
- Automated functionality: TraceCSO made incident response easy to understand and highly automated - eliminating the need to hire additional support personnel for it.
- Depth: The Incident Response module addressed the institution's immediate need to get started without commitment to design a complex and expensive solution.
- Flexibility and scalability: Because TraceCSO is cloud-based, the solution automatically updates and easily scales to accomodate their growth strategy.
- Interoperability: The solution integrates easily with other security applications
- Optional functions: The TraceCSO platform offers seven other functions that can be easily activated.
- Breach expertise: TraceCSO's team not only designed the software, they have been involved in responding to cybersecurity breaches, can provide real-world insight, and are accessible upon request.
- End-to-end functionality: The TraceCSO platform offers seven other fuctions that can be easily activated using the same data as the incident response function. These other functions will allow the organization to manage its risk, vulnerabilities, internal audits, compliance reporting, training initiatives, vendor due diligence, and policies. As the organization's information security program grows, TraceCSO delivers seamless integration, a common user interface, and eliminates redundancy.

Looking Ahead

With incident response functionality in place, the credit union anticipated leveraging additional TraceCSO modules to enhance their cybersecurity capabilities. The fast, flexible, and affordable approach may have addressed their needs for an incident response solution, but everyone agreed that the other modules in TraceCSO could help them proactively prevent cyber breaches.

The C yber JTF's success was a unique first for this institution, and within the year the team integrated additional functions within TraceCSO to help proactively manage and prevent cybersecurity breaches. The fastest, most flexible, and more affordable way to address cyber breaches and incident response is to prevent the breach in the first place, and TraceCSO can do this for them.