Redjack

Financial Services Firm Improves BCDR Planning & Compliance

Uses Asset Inventory to Improve Visibility and Manage Third-Party Risk

INDUSTRY	ASSET COUNT	CUSTOMER SINCE
Financial Services & Insurance	12,000	2016

CUSTOMER CHALLENGE

Compliance & Visibility

The customer was facing urgent regulatory difficulties related to a cyber incident that called into question the reliability of their business continuity and disaster recovery (BCDR) plan, among other things.

Pressing Business Needs

- Identify and analyze the dataflows between assets.
- Prioritize assets by data classification (whether it contained customer data, financial data, etc.) and business value so that they could identify critical business functions (CBFs).
- Identify third-party transactions.
- Identify CBFs that were dependent on external connectivity.
- Find a way to monitor, detect, and automate this process moving forward.

Difficulties With Security Scanner

- It could only identify those assets that responded to communication requests.
- It couldn't identify what each asset was for and what it did.
- It prioritized assets based on age instead of importance.
- It suggested multiple remediations (approximately 800,000 in the customer's case) but didn't explain why each one was necessary or prioritize which remediations were most critical.
- Vulnerability scanning was futile, as it took a day and a half to execute and the data was mapped to IP addresses – which were configured to change daily. By the time a scan was completed, there was no way to identify which specific asset had which specific vulnerabilities.

Business Results

Redjack deployed a series of sensors to internal network aggregation points to generate an asset inventory (prioritized by CBF) that allowed the company to comply with regulations. We demonstrated why it's important to monitor network communications that connect to the internet not only because the National Institute of Standards and Technology (NIST) includes it in their Cybersecurity Framework, but also because it helps to gauge the function and importance of each asset.

Achieving compliance with the New York Department of Financial Services (NYDFS) Cybersecurity Regulations enabled the company to meet additional regulatory standards, such as those required by the California Consumer Privacy Act (CCPA), which a company must abide by in order to conduct business in California.

In the process, we also analyzed network traffic behavior, performed a threat analysis to detect malicious activity, and presented the customer with a list of security improvement opportunities.

Business Continuity and Disaster Recovery (BCDR) Planning

An issue the customer faced related to its BCDR plan — a vague, 24-page document that focused on what the company would do in the face of a physical disaster but lacked provisions for other possible emergency situations. It also contained little information on how to restore assets in the event of a problem or a description of what would happen, logistically and financially, if they weren't restored in a timely manner. Experts were able to revise and improve the customer's plan using the data that Redjack provided.

IT & Cybersecurity Architecture Best Practices

Redjack informed the customer about several serious issues related to the setup of their environment. For example, the asset inventory revealed that phones had been exempted from the company's preliminary asset list, even though they could be plugged into the network. People had also connected their own switches and hotspots, which were not reflected in the inventory.

We also discovered limited network traffic that wasn't using a virtual private network (VPN), which meant public user Wi-Fi traffic and server traffic, which needed to be segmented, were being funneled through the same firewall. Several server applications were also out-of-date, which posed problems for the security of the company's Active Directory (the place where admins manage permissions and network access on Windows servers).

Finally, the customer did not have a configuration management database (CMDB) (an accounting of the company's hardware and software assets). Populating one would have been a challenge, as CMDBs are notoriously difficult to operate and maintain, but the asset inventory Redjack provided was able to fulfill this need.

Third-Party Risk

External Vendors

The customer lacked a comprehensive list of external vendors, such as SaaS providers, that they rely on to deliver their services. NIST principles require financial companies to maintain such lists, as their vendors are subject to the same security regulations as the financial companies themselves and must be audited annually.

To address this oversight, Redjack provided a network diagram identifying the CBFs that were dependent on external connectivity and documented the flow of information to and from those parties. We explained that Redjack's monitoring capabilities provided a way for the customer to better detect external vendors, and we supplied a list of the 10 vendors that were exchanging the most data with their network. The customer was unaware they were working with some of the names that appeared on that list.

Confidential Data

At the time, the company outsourced their IT overseas. The company had paid to construct a brick-and-mortar facility in India so that contract employees could work with confidential information and other data subject to regulatory oversight within a secure environment. In monitoring communications throughout the customer's network, Redjack detected that there were communications connecting to and from India through a VPN. It turned out that some employees were choosing to work from internet cafes instead of the specially constructed facility. Redjack also discovered that select 1099 contractors were personally outsourcing work and sharing account credentials without the company's knowledge. While Redjack didn't observe any breaches in the related communications, the situation did result in litigation.

Network Segmentation

The company wanted its security staff to be able to walk around with access to camera feeds on tablets. Doing so relied on the use of Citrix, a connectivity platform that cannot be segmented. We pointed out that with this setup, anyone able to get into the customer's environment would also be able to access physical security assets, like cameras and alarm systems. Both are forms of operational technology (OT) that connect to the network but aren't traditionally thought of as computers, so people fail to patch and segment them, leaving them vulnerable. As financially regulated environments need to be segmented, the CISO and CIO recognized this access as a problem that needed to be addressed.

Conclusion

Using the intelligence that Redjack provided, this company has been able to improve not just its regulatory compliance and its BCDR plan, but much more. In addition to the original scope of the project, Redjack was able to help the customer identify several areas where they could improve their architecture, including network traffic that needed to be segmented and controlling access to OT assets. The customer was also able to identify several areas of third-party risk that they had been unaware of so that they could correct it. Overall, by working with Redjack the company was able to improve not just its regulatory compliance, but its overall cybersecurity posture.

About Redjack

Redjack delivers total asset visibility and AI-powered business insights for cyber resilience. Our platform empowers enterprises to safeguard vital business functions, meet cyber regulatory standards, and digitally transform to align with business objectives.

Visit redjack.com