proofpoint.

Bank Assesses Identity Risk With Proofpoint to Complete M&A Safely

The Challenge

- Assessing the security posture of another bank they are acquiring
- Finding identity vulnerabilities—when they had no other solution
- Tight and inflexible deadlines for the closing of the acquisition

The Solution

Proofpoint Identity Threat Defense
- Proofpoint Spotlight

The Results

- Full identity assessment of the acquired bank in less than 30 days
- Discovered thousands of critical identity risks that were completely unknown
- Concrete, quantitative data persuaded executive team to delay full IT integration until issues were addressed

The Company

The company is a United States regional bank holding company with about $200 billion in assets. Founded over 150 years ago, the bank and its affiliates provide consumers, small and middle-market businesses, corporations, municipalities and other organizations with a comprehensive suite of banking and other financial services. The company has about 25,000 employees and operates more than 1000 branches.

The Challenge

The company operates in an industry where consolidation is the norm. Over the last 20 years, the number of FDIC-insured commercial banks has dropped almost in half, primarily because of acquisitions. In this bank's case, they've been averaging an acquisition every three years. Each time they've gone through the process of a merger and acquisition (M&A), their IT department has needed to consolidate different systems, software, data, processes and organizations.

If any bank acquires an organization with a weaker IT security posture—or even one that's unclear to them—it can put the company at risk. Conducting a security assessment is critical, and often it needs to be done under tight time constraints.

As the bank's director of cybersecurity engineering says, "We had at most four months, from the announcement of the transaction to the closing, to evaluate the other bank's IT security posture. We needed to know if we could trust them."

"I'm glad we used Identity Threat Defense. Everyone saw the value. It's a playbook we'll carry forward through the next M&A."

Director of Cybersecurity Engineering

The Solution

Since identity security underpins their entire security posture, getting an understanding of potential identity vulnerabilities at the acquired bank was critical. As a Proofpoint customer, the acquiring bank was familiar with the solution and highly valued its insights. "We'd been using Proofpoint to continuously scan our workstations for six months or more, so we were familiar with the insights it could provide."

The Results

The evaluation of the acquired bank was critical in producing a risk scorecard comparing the two IT organizations, and in this case, there was enough risk to convince executives that the IT environments needed to be kept separate, at least initially.

Although there were several identity risk areas, one quickly jumped out. "The smoking gun was the number of domain admins on their workstations. There were 3,000 of them. It just showed the state of their security hygiene. Anyone compromising one of those workstations would have had control of the whole environment. They didn't know about it either, so they worked on cleaning that up."

The overall results of the comparison were compelling. "It would have been a much more difficult discussion without the pre-integration identity risk scan—to justify the increased protection we felt we needed at that initial point."

In addition to M&A situations, the bank uses Identity Threat Defense to continuously scan its own environment for identity vulnerabilities. This is part of a complete solution that includes Qualys, Kenna, ServiceNow and other solutions for threat and vulnerability management.

Asked about the future, the director says, "I'm glad we used Identity Threat Defense. Everyone saw the value. It's a playbook we'll carry forward through the next M&A."

LEARN MORE

For more information, visit **proofpoint.com**.

proofpoint.