cybertrust

Growth by Acquisition Brings Security Challenges to the Financial Services Sector

MSS Case Study

Industry: Financial Services

Situation: Managed Security Service—Cybertrust OnlineGuardian®
Monitoring and Management
Transitioning over time to SOC On-site

A large financial institution was growing quickly by acquisition. In fact, it was buying a company a month—which posed a significant challenge when it came to securing the data of all its new entities. First, the company needed to get each new acquisition up to the same security standard as the rest of the organization. Second, it needed constant visibility on the status of its security, in case of a breach. The company effectively had two options:

a) To build an in-house Security Operations Centre (SOC). This was certainly an option for the future, but given the rate of acquisitions and the cost of putting it together, it was not currently feasible.

b) Fully outsource security considerations, which was a far more sensible idea in the short term.

After completing its analysis, the company approached Cybertrust, which offered the flexibility of Managed Security Services now and the expertise to build an in-house SOC on-site later on—when the acquisitions had tapered off and it was time to bring security in-house.

Consistent Security in an Ever-Changing Environment

Sites Up Quickly

With Cybertrust Managed Security Services, the new acquisitions were efficiently integrated and brought up to the required level of enterprise security within weeks—which meant the company immediately benefited from a consistent security level that was commensurate with its business risk.

Integrated Intelligence

With more than one million threats and alerts occurring daily, it was a nightmare to decipher what was real and what wasn't. But with Cybertrust's SEAM™ (State and Event Analysis Machine) technology, the company didn't have to worry. Now, they are only alerted to those threats that pose a real business risk.

Visibility on Costs

With Cybertrust's Managed Security Services, the company can view all its costs on a monthly basis (which were 4 times less than if it had implemented its own SOC), and the company is protected by a Service-Level Agreement it can count on—because it's external, rather than internal.

Demonstrate Compliance

Cybertrust also gave the company the ability to achieve and demonstrate compliance with a number of industry standards through its COBIT 4.0 framework—bridging the gap between control requirements, technical issues and business risks and serving as an independent third-party validation of the organization's security measures.

cybertrust

Expert Vendor Knowledge

Cybertrust also offered expert knowledge and advice on all the different vendors and products. With so many acquisitions and sites, it was advice that has helped the company keep on top of everything out there.

Follow-the-Sun Protection

With SOCs and Security Management Centers around the world, the company is protected 24/7, 365 days a week.

Healthy Devices

Cybertrust monitors the CPU load and memory load of every device, every 10 minutes—helping to build a proactive and predictive security model that alerts the company when devices need to be fixed or replaced.

Easy to See Security

The tool that ties it all together is the Security Dashboard—an intuitive web page that allows the company to see at a glance what its security posture is. Security Managers can show the CIO how healthy devices are and which logs and alerts require attention. It also enables the company to centralize change management controls and acts as a powerful authentication and authorization model.

Someone to Represent You

The client felt that SOC contacts could be too technical, and wanted someone to turn to whose primary objective was to make sure they were looked after. The Cybertrust Client Services Manager (CSM) was that person (a role not many MSSPs have). CSMs are responsible for delivering the SLA and following up on all customer requirements and requests. They also serve as the escalation manager.

Cultural Adjustment

As a large organization, the company knew the benefit of good policies and processes—but it had a very entrepreneurial culture and knew, too, how cumbersome they could be. The reality, however, is that security management has to be thought through—which means things slow down. With Cybertrust, the company was able to educate fast-acting business managers about how to plan ahead, so changes to security policy ran smoothly.

Getting the House in Order

It's a real challenge to inventory all the assets sitting behind security devices, figuring out what needs to be protected, from individual PCs to application servers and databases, how many there are, and how they are linked. Cybertrust helped the company inventory the primary site and then all subsequent sites through electronic scanning and on-site assessments during the set-up phase.

Moving Toward the In-House Solution

In the future, as the acquisitions start to dwindle and the organization becomes more established, the intent is to build an in-house SOC. The company knows that Cybertrust can help with costs, staff, technology and processes—and will also provide its powerful SEAM™ technology or work with another Security Event Management tool.

cybertrust

Business Benefits:

1) Enhanced security posture.
2) Specialized, objective advice.
3) Guaranteed compliance with most industry standards.
4) Easily enforceable SLA.
5) Predictable monthly costs.
6) Optimization of existing investments in technology and people.
7) Ability to grow and change to the SOC On-site, a more relevant service, in time.

Technology Benefits:

1) 24/7 monitoring that is too expensive in-house in the short term.
2) Overcome information overload—hundreds of millions of logs and alerts deciphered on the company's behalf.
3) Retain the best practices of a diversifying technology portfolio, without having to know everything about each product or vendor.