Outsourcing IT Security Options

cyber security risk management

Summary: When should community banks outsource IT security measures? We have some answers.

The world's most popular websites according to the World Economic Forum are Google, YouTube, Facebook, Baidu and Wikipedia. Given how much people use the internet, no matter the website, risk has increased.

It can be difficult and expensive to develop an in-house cyber security team. This is true, in part, because of a nationwide shortage of cyber security talent. For community banks, outsourcing IT security can be good but it also can increase risks.

As you think about whether and when to call in IT help for your teams, you will still need in-house capabilities. To begin, ask how complex your IT environment might be and fit that to the skills of your technology team. The more locations, servers, devices and access points you have, the more complicated the necessary security arrangements will need to be.

Another thing to consider here is whether your bank is easily handling regulatory and reporting requirements, or whether such tasks are taking up a disproportionate amount of staff resources and time. Then you can determine the best way to proceed.

In the case of a natural disaster, it is important to recover quickly. To do so, you need to recover facilities, data, and customer access points as you manage and monitor branch systems as things get back to normal.

In addition to this, bankers are fearful and dealing constantly with cyberattacks. Having confidence in a team is one thing, but doing penetration testing, having more targeted audits and other factors can help ensure expectations meet reality.

Security monitoring is one of the services most commonly outsourced to a third-party provider. If your bank lacks the budget or personnel to handle comprehensive monitoring and security alerts, this is a place where a vendor may add value.

Once your security monitoring is covered, you'll want to consider what you'll do if and when you have a real security incident. As part of your preparation for that possibility, you may want to establish a relationship with a vendor that specializes in forensics and incident response. Having their number at your fingertips in the heat of a crisis can make the difference between a stumble and a coordinated, logical response.

Third-party security testing is a best practice, if your bank develops some of the IT-based services and products it offers customers, and may be a compliance requirement. Though you probably do your own testing as well, there's no substitute for an outside firm with the objectivity and expertise to really push network penetration testing, application security testing, and product security testing.

Third-party assessments can also mean asking a vendor to examine the security measures taken by other vendors, an acquisition target, or business partners. This is a chance to see another company's potential security gaps through a new set of eyes, before those risks complicate your own security fabric.

Training is also critical and is often ignored or glossed over. Here, we suggest doing targeted training for specialized functions to enhance knowledge. A specialized trainer can teach staff how best to protect the bank and stay focused on issues they are most likely to see in a given position.

Outsourcing some technology tasks may more efficiently help you manage cyber risks and allocate your resources, but it can also add risks. So, care and diligence must be used. Be selective and carefully vet all vendors diligently, as this is an area where you cannot afford to see critical mistakes.

OUTSOURCED ALM SERVICE FOR COMMUNITY BANKS

Managing interest rate risk is both art and science. Regulators have raised the bar and community bankers have more to do than there are hours in a day. To see how easy it is to outsource & get expert help, contact us today.