THE INVISIBLE RISK – NETWORK SECURITY

What you can’t see can’t hurt you, right? A perspective for nontechnical bankers

• • •

By Peter Graves, CIO, Independent Bank. Graves has 25 plus years experience on the business side relating to commercial lending administration and on the technology side in his role as chief information officer for Independent Bank, a $2.7 billion community bank with over a 100 locations in the lower peninsula of Michigan.

How many of you have experienced some kind of risk buried within your institution, invisible to you and your team that was just waiting to rear it’s ugly head and bite you? As an industry, financial institutions have been faced with the underlying and seemingly invisible risk within lending that was overly dependent on real estate values as the second source of repayment. The lack of visibility relating to this risk caught everyone off guard and has changed lending as we know it forever. Again, not because the risk was unfamiliar to us, but because it was systemically woven within our loan portfolios, un-aggregated, and less visible from a risk perspective.

Likewise, there are hidden or invisible risks that lurk within the corners of your IT network waiting to be exploited. These also are risks that potentially could change your organization forever. It only takes one flaw or one vulnerability that could expose your institution to hundreds of thousands of dollars in investigation, mitigation, and legal fees, not to mention the time and resources spent to recover from it.

Relative to information security, the financial services sector continues to be the second most targeted industry in the world. According to the Verizon Business 2009, 2010 Data Breach Report (a joint effort with the United States Secret Service), 98% of all data breaches come from servers, 86% were evidenced in existing IT log files, and 96% could have been avoided through simple controls. Startling statistics for most bankers who just want to know that their laptops will boot-up and connect to the network every morning. Those invisible risks are just not front-of-mind.

Mobility has changed everything

Traditionally, most of us think of our network security as a “moat or wall around our castle.” “Firewall” is a common term in IT that establishes a bright line between that traffic that is internal to our network and that traffic that is external. Traffic or data must pass through a set of security or business rules to qualify as safe, most often specified within the firewall software or firewall appliance. But it is really nothing like a moat or wall. Today, thousands of devises are connected to our network, from servers, routers, switches, and printers, to smart phones and even iPads. Mobility in the workforce, in particular, has changed everything. You need to adjust your paradigm relative to security and think of it as more end-point security rather than a moat or wall around your perimeter. Each end point or device poses a risk to information security. For that reason, security to protect our data and information is much more difficult today than it was ten years ago.

Exposing what is invisible

So how do you expose what you can’t see? As I mentioned earlier, 86% of threats were actually evidenced in existing IT logs. These logs are audit trails of events and data that traverse and transact across the network. Servers, routers, switches that are the cornerstones to network infrastructure produce logs along with many network enabling software systems that support and help manage the network. Conceivably on a given day, there may be tens of millions of log events that could potentially signal a threat or breach. How could a typical community bank security team of one or two network engineers possibly sift through all those events? In the not-so-distant past, that is exactly how threats were analyzed, by physically reviewing log reports. As our network complexity has grown, our methodology to combat these threats has also had to evolve.

Today, there are many tools available to assist with the detection and prevention of data breaches. These are less costly and more effective than just hiring more IT staff to maintain and monitor devices. There are security modules that detect and often sit on core switches or firewalls and sniff packets of data that flow in, out, and around the network. These devices or tools are known as Intrusion Detection Systems (IDS) or Intrusion Detection and Prevention Systems (IDPS). The difference being, IDPS systems are more proactive in disabling or blocking these offenses once detected. This may or may not be advantageous depending on network interdependencies and systems complexities. Often, recognizable offenses can take milliseconds to become threats. Automated blocking or disabling may be critical to successful containment of the threat. Multiple IDS type systems that are tied to other network devises such as servers, routers, switches, firewall appliances, proxy devices, etc. produce logs or audit files for eventual review.

Algorithms comb through millions

Like searching for the proverbial “needle in a hay stack”, how does security resources filter all the sanctioned events from the undesirable offenses? Entire security programs known as Security Information and Event Management (SIEM) systems have been developed to assist with finding the invisible “needle.” Platforms as tools have been refined over the years to assist security staff to isolate and manage offences. These tools use highly sophisticated statistical algorithms to correlate millions of events whether they originate within or outside the network. The interrelationships of those events generated are then boiled down into a few highly probable and actionable offenses that might require more research by IT staff. In a given day where ten million network events are generated, ten events might warrant further investigation (a million-to-one compression). Platforms by Cisco, Q1, TriGeo and others are instrumental in staying a step in front of these potential threats while decreasing the required physical resources to manage them. These solutions truly help to uncover what is buried or invisible within the data traffic that navigates through the network on a daily basis.

Seeing is believing

If you never see or hear of an information threat or data breach, your existing security staff and solutions are either exceptional or the threats are there and undetected and it is only a matter of time before those threats materialize into a real event. Often, within days of implementing these latest SIEM platform solutions, risks or threats become known that can be addressed and then remediated before exploitation. Again, seeing the output of a proven SIEM solution can make you a believer in the technology. They allow an institution to control costs while keeping up with the ever evolving and increasingly complex nature of network threats whether they are internal or external. If an institution can identify the risks, they are more than likely able to contain them with simple controls. Again, as I mentioned earlier based on Verizon’s report, 96% of all threats could have been avoided by simple controls.

Outsourcing pros and cons

So ask your IT security staff these questions:

• What types of IDS devices do we deploy?

• How are the event logs that are generated filtered, correlated, and managed based on all the potential offenses that occur everyday?

• What is our SIEM program?

That will get their attention. You will either receive a warm smile for your interest or be arrested on the spot for asking suspicious questions.

But seriously, are they outsourcing their SIEM program to determine what a potential threat is and what is not? Outsourcing has proven to be a reliable alternative since the providers typically invest and implement the latest in detection and prevention systems so the bank does not have to. Unfortunately, the latest and greatest comes with a hefty monthly bill. The outsourced solutions often leave significant gaps between those security activities that cannot be outsourced and those that are provided by the vendor.

Whatever the security solution is in your institution, make sure it is emphasized as one of the top initiatives in the company. Today, emphasis on security resonates positively with customers and employees. Remember, risk does not have to be visible to be a real threat.

Closing thoughts

And finally, all the best security systems and tools can not take the place of physical and individual preparedness; being alert to sudden changes in the digital environment we call our “work place.” Support the efforts of those dedicated to an ever-changing and difficult task of information security. Celebrate those risk events that are prevented and learn from those that aren’t. Invest in your people. Training and awareness could prevent the unthinkable, a data breach at your institution.

We hope you find this new blog helpful. Please send suggestions for IT and bank technology topics you’d like to see Pete Graves deal with to scocheo@sbpub.com