Five Considerations for Securing a Midsize Company

http://searchSecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1349701,00.html
by: Marcia Savage
Issue: Mar 2009

Get creative.

That's the most important step for anyone in charge of securing a midsize business, says Tony Meholic. He should know. Meholic went from managing the ethical hacking team at JP Morgan Chase, a huge worldwide enterprise, to leading security at Republic First Bank, a 300-employee regional bank based in Philadelphia. At JP Morgan, buying a $100,000 tool was a simple matter of some paperwork and signatures. At Republic First, asking for a $25,000 tool got him a pat on the back and a vague promise of "maybe sometime."

"You have to get more creative as far as maintaining security, because certainly the requirements don't change," Meholic says.

Just like their large counterparts, midsize companies with 100 to 1,000 employees face regulatory compliance pressures. They also face the same kinds of threats and can't afford a reputation-destroying and costly data security breach. But unlike big enterprises, midsize businesses don't have the luxury of ample resources and large security teams. They rely on ingenuity to figure out ways to secure their data assets on sometimes shoestring budgets and are well-versed in the resourcefulness the recession requires of companies of all sizes.

For Meholic, security on a tight budget led him to automate and streamline manual processes. Security officers at other midsize companies and industry experts cite automation as a key tactic, along with other strategies, including wringing more security value out of existing equipment and outsourcing certain security services. Some point to core strategies applicable to businesses of all sizes like risk management. We've compiled their advice into five essential considerations for securing a midsize business.

1. Risk management

For many companies, including midsize ones, smart security starts by analyzing and assessing risks.

"Step one is to figure out what your risks are," says Matt Roedell, vice president of infrastructure and information security at TruMark Financial Credit Union, 300-employee firm with $1 billion in assets based in Trevose, Pa. "You need to perform a risk assessment."

Once a company does a detailed risk assessment -- either on its own or with outside expertise -- it can analyze which risks impact its business the most, research what tools and services can mitigate them, and how much those solutions cost, he says.

"It's very easy to put a proposal on a desk and say, 'We need this.' It's different when you put it in terms of risk to the business," Roedell says. Along with a proposed purchase order, he recommends presenting business executives with what he calls a "risk acceptance document" in the event they don't want to fund the risk mitigation. No one will want to sign it, he says.

Business managers aren't IT or security experts; they just want to know what will negatively affect the company and its bottom line, he says: "So tell them what it will do to the bottom line."

Indeed, midmarket information security managers must take the time to understand their company's business,

especially in these tough economic times, says Khalid Kark, principal analyst at Forrester Research.

"You need to pick your battles. You have to prioritize," he says. "To do that, you need a clear idea of what the business priorities are and what your existing capabilities are."

Instead of creating a laundry list of security actions, those in charge of security at midsize companies should step back and look at what parts of their business are most critical, e.g., if it was lost how much revenue the company would lose, says Jack Phillips, co-founder and CEO of IANS, a Boston-based infosecurity research firm.

"You can't cover all your risks. You have to make an educated guess as to where your highest risks are and focus on them," he says. "Prioritize is the key word."

In a down economy, companies need to view their business processes from a risk perspective and look at ways they can reduce risk by re-architecting the process instead of buying more products, Phillips says.

Jay Arya, a vice president and information security officer at Short Hills, N.J.-based Investors Savings Bank, which has about 500 employees including three focused on security, says any business must take a holistic approach to information protection. For example, email security can't be implemented without taking into account its impact on business processes; if it winds up blocking email to customers it would hurt the business. At the same time, sensitive information needs to be protected, he says.

"You have to look at the whole company What the business needs are and focus security based on that," he says. "The last thing you want is your business to suffer because of security. It's a fine line between effective security and operation of the business."

All-In-One Security

UTMs can streamline security, but aren't a cure-all.

FOR MIDMARKET COMPANIES without a staff devoted to security, unified threat management (UTM) devices can be a good option. These products combine security functions such as antivirus, intrusion detection and firewall protection, forming something of a security Swiss Army knife.

"It's less costly to manage and it usually has a single interface, so there's less training required. One person can manage it," says Jay Arya, a vice president and information security officer at Investors Savings Bank.

While an all-in-one device can streamline security, it can have its drawbacks -- namely that it may not do everything well, he adds. "It may not have the correct features to enable the tight security some users may need."

A UTM is a good fit for certain situations, depending on what security problem a company is trying to solve, he says. The multi-function appliances can be helpful with certain functions, such as antivirus, antispyware and firewall protection. At Investors Savings Bank, a UTM from Sophos, Sophos Endpoint Security and Control, allowed it to combine those functions onto a single platform, making them more efficient and easier to manage, he says.

Tim Richardson, security products manager at IT services firm Akibia, says the power of technology has increased over time, making it possible to do more on a single device. Having a firewall, IPS and antivirus on one device is easier to manage but has the potential to complicate troubleshooting, he says.

"You have to make sure your troubleshooting tools are robust enough so whatever happens, you can pinpoint it," he says.

--MARCIA SAVAGE

2. Automation

Midmarket companies often rely on one person to manage security, and in many cases, that person juggles security responsibilities with other work. Limited manpower can make automation critical in the midmarket.

"You have to get creative about the use of resources," Meholic says. "The more you can automate the better."

Forrester's Kark says some midsize businesses actually are a little more advanced in their use of technology compared to big companies, so they take advantage of the automation it can offer. "They don't have a lot of resources and typically technology and automation of some tasks would enable them to keep that low level of resources and still be able to do at least adequate security."

One particular area where automation can help is compliance; there are a slew of tools that gather, analyze and report on compliance activities holistically instead of doing each activity individually, Kark says.

Arya at Investors Savings Bank says his firm's regulatory requirements include FDIC, SOX, GLBA, and state rules, making compliance a huge task. He's evaluating a tool that would provide automatic compliance reports.

"To comply with all the different regulations, you need to understand them and understand how they affect customers and the business," he says. "An automated tool makes it easier to set a preset model, feed the data into it and it provides reports, which makes the auditors happy."

The governance, risk and compliance (GRC) tools he's looking at don't come cheap; they range in price from $20,000 to $100,000. Depending on what a firm wants to achieve, spending $30,000 on a product to automate compliance makes sense if it means it doesn't have to hire additional personnel, Arya says.

For Cimarex Energy, a tool from Guardium provides automated database security monitoring that goes beyond the ability of a human. The Denver-based independent oil and gas exploration and production company, which counts about 850 employees, has an ERP application that processes about a million database transactions an hour.

"At that rate, there's no way you could have a human doing any kind of monitoring," says Ann Auerbach, manager of IT compliance at Cimarex. "Auditors always ask how you know the IT staff isn't going in at night and changing the data Without the tool, I don't know how we would prove to the auditors that unauthorized transactions were not entered into the database."

The tool also helps IT staff at Cimarex locate problems such as infected PCs by tracking unusual activity such as invalid database logins, she adds.

For Roedell at TruMark Financial Credit Union, the automation offered by security information management (SIM) technology is essential; his company uses a SIM product from TriGeo. What makes an infosecurity program effective is the ability to analyze all the security data in the environment in real time and take action, he says, adding "The only way to do that is with a SIM."

In some cases, automation doesn't have to require extra investment in technology. For example, Microsoft Excel spreadsheets can be customized and programmed to automate a lot of tasks, Meholic says.

He leveraged Excel when he automated and integrated several manual processes at the bank. User access

reviews, IT risk assessments, GLBA assessments and other processes were all tediously manual, he says. He conducted a data flow examination to identify assets that interacted with confidential information; applications could then be assigned a "confidential data footprint" or CDF value. Those values are used across the various processes, so that employees don't have to start from scratch with each process and also for rating consistency. A change to a CDF is automatically made in spreadsheets for all the processes, reducing maintenance time and improving resource efficiency.

"It doesn't have to be anything really elaborate," he says. "There are a lot of things like that that can make life easier."

Deployment: One Step at a Time

Phased approaches to IT projects are popular in the midmarket.

AN INCREASINGLY popular strategy for some midsize companies is a phased approach to technology deployments, says Khalid Kark.

"They're forcing vendors to provide them with modular solutions," he says. "So identity and access management could be a multi-year project. They're asking vendors to provide a step-by-step, modular approach."

This approach allows a company to break up large projects that require a lot of time and money into chunks and periodically re-evaluate the project's status, he says. "So every year, they go back and re-evaluate where they are and where they need to go from there."

For example after the first year, a business could decide the investment is too much and hold off on taking additional steps, Kark says. "They want the flexibility to be able to change course when necessary."

--MARCIA SAVAGE

3. Leveraging existing infrastructure

Figuring out ways to get more security from existing technology is a money-saving measure that many companies have started to consider in order to weather the recession, but the tactic can be essential for perennially resource-strapped midsize companies.

"There are so many things you can do to reduce risk by just using what you already have," says TruMark's Roedell.

For example, organizations can simply turn on the built-in port security in Cisco switches, he says, explaining that port security is critical for preventing just anyone from walking into the office and plugging in a laptop. "It doesn't cost anything but labor to turn it on," Roedell says.

Tim Richardson, security products manager at IT services firm Akibia, says the company focuses on educating customers about leveraging their technology investments in order to get the fullest benefit. Westborough, Mass.-based Akibia serves a client base that is about 50 percent midsize businesses.

Data leak prevention is one area of security that can cost a lot depending on what a company wants to achieve, but businesses can reduce their risk of data loss substantially by simply using the Transport Layer Security (TLS) encryption feature that's included in most email gateways, he says.

"Where is most of your data coming and going? That's email. Chances are the bulk is between you and partners You probably already have a contractual relationship in place with them. You just need to make sure the email between the two organizations is encrypted," Richardson says.

"The technology is there, it's just a matter of taking time to validate it works," he adds.

With security technologies such as firewalls maturing and becoming integrated parts of the network infrastructure, companies are more willing to have one vendor provide multiple functions, says Forrester's Kark.

"Midmarket companies are a lot more open to that," he says. "Many infrastructure vendors are adding on security components and midmarket companies are more open to adding the security components as opposed to buying something new," Kark says.

IANS' Phillips says another strategy that can be effective for midsized companies is one large enterprises are using: turning vendors into partners.

"If you have an incumbent security software provider, alert them that your expectations will go up that you will expect the best thinking from them on not just how to lock down firewalls, but how to reduce the risk exposure for the enterprise," he says. "They can be a free resource to draw upon. Their incentive is to help you because they don't want to lose your business."

And of course, organizations can reap a lot of security benefits with simple policy implementations, such as preventing users from acting as local administrators on their PCs, Roedell says. Acting as a local administrator allows an employee to install programs on a machine, which can lead to a host of security problems.

4. Managed services

Over the past year, Kark has seen a sharp shift towards managed security services. While the economic downturn may have accelerated this trend, managed services can be a good option for companies with limited security expertise on staff, he says.

"I'm seeing a lot more midmarket companies moving to outsourcing of security operations and services. It's pretty useful for a company that's resource constrained to hire an outsourcing company," he says. "It won't save money but what you get is a lot better protection and 24x7 support."

The biggest value from outsourced security is the expertise, which is in short supply; companies pay a premium to have that knowledge in-house, Kark says.

Arya agrees that expertise is the top benefit of a managed service, but adds that outsourcing can also eliminate hardware costs and streamline reporting.

"Midsize companies don't have all the resources to handle every single aspect of security," Arya says. "For those, managed security is not only a viable but necessary option. These companies have the tools, the resources and the expertise."

Kark says some managed security services such as firewall management, vulnerability management and antispam filtering are more mature; it's easier for a midsize company to know what it's getting with those services and their associated costs when it shops for an outsourcer.

But outsourcing doesn't mean entirely hands-off. Vendor management is important, Meholic says.

For instance, when Republic First uses outsourcers for vulnerability assessments or penetration tests, he makes sure the way vendors rank vulnerabilities matches with the bank's criteria, he said. Vendors can have a tendency to rank the severity of a vulnerability a bit higher than an organization will, he adds.

"They are working for your, so you need to make sure you control how they do it and how they report it," he says.

Other midsize organizations prefer to rely on their in-house expertise. Cimarex's Auerbach says the firm is very selective when it comes to outside vendors for IT projects; preferring to use the knowledge of its 40-member team of seasoned IT professionals. The small size of the team also facilitates cooperation, and makes it easy for employees to pick up the phone and call a colleague to analyze potential problems.

"If it looks like we're getting a lot of unsuccessful login attempts, it's easy to respond because we have such a small group," she says. "You can easily pick up the phone and ask, 'Can you take a look at this?' and get to the root cause in very short amount of time."

Numbers: SMB Security Priorities

Forrester Research survey of North American and European companies highlights top issues for midmarket companies.

- 87 percent deem data security as important
- 61 percent say other organizational priorities taking precedence over security is their top challenge
- 31 percent cite demand for specialized skills as the top driver for using a managed service
- 58 percent have deployed personal firewalls
- 19 percent plan to adopt or pilot a host intrusion prevention system this year

Source: Forrester Research

5. Security awareness

No matter a company's size, training employees about information security is critical. The human element is by far the biggest risk in an organization, says Mike Helinsky, director of information technology operations at Brooks Health System in Jacksonville, Fla.

"The person who leaves their user name and password on a sticky note attached to their monitor That is by far the weakest link in the entire security spectrum," he says.

For midsize companies, it's particularly important to educate not just the rank and file about security but also executive management, Kark says. The recession -- which can increase the potential for insider misuse of systems but also lead businesses to take on more risk to save money -- makes this education more critical, he says.

He's seen several cases in which those in charge of security at midsize companies have made convincing arguments to executive management about the need for security by pointing out the costs of a breach and how they could potentially put the company out of business.

One of Arya's first steps when he took the security leadership role at Investors Savings Bank was to roll out an online security awareness tool for employees. Awareness is key for all users, no matter their position, he says.

"These days, in any business, if everyone doesn't get involved, security is not going to work," he says.

Republic First puts a priority on security awareness training for employees as well as its customers, Meholic says, noting that the federal Red Flag rules require financial institutions to provide security training for employees and customers.

Moving forward, though, he'll have more help in securing the organization. Late last year, Pennsylvania Commerce Bancorp acquired Republic First Bancorp, the holding company for Republic First Bank. The newly merged company, Metro Bancorp, counts more than 1,200 employees and Meholic expects it will have a staff for

information security. While the basics of his job will remain the same, there will be some challenges, he says.

The first challenge will be making sure the bank's established infosecurity program meets the needs of the new, more complex environment, Meholic says. To that end, the infosecurity team's main focus will be identifying any deficiencies and developing new policies and processes to address them. The next challenge will be to have a well-defined role for the team.

"Once established and integrated with the other departments of the bank, performing information security related tasks should be easier," Meholic says.

Marcia Savage is Features Editor of Information Security. Send comments on this article to feedback@infosecuritymag.com