CORNERSTONE SOLUTIONS
IDENTIFY. PLAN. SOLVE. SUCCEED.

The 5 most important security questions every company needs to answer

As you have probably heard several times over, data security is all about layers (and don't forget risk)! In our June 2018 webinar on security, I included this quote from David Britton, Global Vice President Industry Solutions/Fraud and Identity at Experian:

"The truth is that since 2013, the [amount] of breach activity is so large, we assume that everyone's persona, everyone's identity data has been compromised, full stop."

In preparation for this article, I thought I would throw together a list of data breaches just to try to put a number around the total data records compromised, but the list was around 9,000 lines (since 2005). And that wasn't even a complete list of data breaches. With breaches including multiple (and sometimes millions) of data records each, it is not hard to agree with Mr. Britton's assumption!

Doing the basics right

A review of any list of data breaches is going to reveal certain patterns. What security researchers have found is that more than half of breaches could have been prevented by diligent adherence to basic security measures, such as patching your computers promptly. In other words, if you get the basics right, you are more than halfway there.

Still, security strategies should be based on risk. You don't want to invest the time and money to secure everything as if it were Fort Knox – it doesn't need to be. So we've put together the 5 most important security questions you need to ask, then answer – for your company. After you have your answers you just need to put the basics in place for everything, and step up the security on the high-risk stuff. Although it does take a little time to get there, we've seen this recipe work superbly for most companies.

For questions 1-4, you don't have to be a data security person to obtain the answers, but ultimately this is a security project - especially when you get to #5 - so you'll want to work closely with whatever data security personnel you have. In the very least you will probably need the IT department's assistance with the first 4 questions, so it will pay off big to foster a good partnership with the appropriate people right from the start.

#1: What is my data?

Before you attempt to tackle this one, check with the IT department as they may have some or all of this documented already, but you'll want to make sure this documentation is comprehensive, complete, and up to date before you use it.

If you need to update it or start from scratch, here are some examples of things you might list:

- Payroll data
- Product data
- Investment data
- Trademark data
- Legal data
- Schematics
- Employee data
- Travel data
- Device data
- Network Configuration data
- Communications data
- Other company's data
- Marketing data
- Network health and performance data
- Backups

This goes hand-in-hand with the next question on where it is stored. In order to assess the risk and protect it, you need to know what data is under your jurisdiction, *at all times*.

You will need to assess each department. Then consider the hire to termination process and what paperwork and duties employees perform between the two. You can work back and forth with your list of storage locations to add to both lists.

#2: Where is it stored?

Here are some examples of things you might list:

- HR Systems, including payroll portals
- ERP systems
- Company Intranet
- Website and Social Media
- Servers
- Software as a service (SAAS) – your data in the cloud, including sanctioned and unsanctioned applications
- Dropbox or other cloud storage, including accounts set up by employees
- Desktop and laptop computers, including personal files for things like Email, and also reports (from Excel or Access)
- Other employee devices
- Disks, USB drives, and employee desks
- File cabinets
- IT support and infrastructure systems
- External media (such as backup tapes)
- Employee's personal devices, including home computers

A good exercise is to talk to employees about the processes they perform from start to finish, and you will discover all the ways they are augmenting those processes by moving data to places you might not be aware of. As a bonus, in documenting these conversations you will be 90% done with all job descriptions and enterprise process documentation!

That said, if your company has a thousand employees (or more) do you have to talk to each one? No. Try to talk to at least one person in each department though. Ask the people you talk with about other processes they are aware of. And try to talk to as many as you can – you never know who is using that group app in the cloud on the side (and not removing access for terminated employees) unless you ask.

#3: What is the risk of exposure/loss?

Next, you are ready to take a swing at listing the risk of loss or exposure for this data (and the hardware it resides on). If security is not in your job description, make sure to talk to your security personnel to get examples of threats and consequences. List each alongside your data and its storage location. Rate or rank each risk based on the sensitivity, criticality, likelihood of loss/exposure and impact to the company to replace it. Try not to rank everything as high risk – simply because it's not.

At this point, you will be cross-eyed. Documentation is never easy, or very fast. But the good news is, once you get to this point, it gets a whole lot simpler. One lunch and learn session with the whole group of enterprise stakeholders and you should be able to determine your company's risk appetite. Beam your list (table, matrix, or however you have it to be presented) up on the wall and promote healthy discussion on each item. Again, try not to make everything high priority, urgent, or a dire necessity. Really listen to your stakeholders and address their concerns, as ultimately the responsibility to protect data does belong to them. If there are items you think are not being addressed appropriately,

you can work on bringing more awareness to them in the next assessment. Do what you can to move forward and get the basics in place first.

#4: Who has access to it?

By now you have process information, what data each person needs (or at least an estimate), its risk ranking and where it is stored. Now, obtain a list of all the people who have access to it.

- If terminated employees are still on the Access List, talk to the appropriate people about implementing or tightening up the termination process. Usually access lists are reviewed at least quarterly to ensure you catch anything that might be incorrect.
- For the employees who are still active, do they all need access to the data (considering its risk ranking)?
    - If they don't need to have access for their daily jobs, remove them. You can always grant access back again later
    - Do they have more access than they need?
    - How many administrator accounts are there? One regular administrator and one back-up administrator are usually all you need
- Have you set up profiles or roles? This will help you review and assess permissions easier
- Is there a formal process for approving and reviewing access on a regular basis?

Whatever you do, don't base access requirements on management hierarchy. Because senior management has historically been given the "keys to the kingdom" so to speak, they are high priority targets for hackers. In typical enterprises senior management doesn't need access to anything but reports.

#5: How do I protect it?

Because they are targets for scammers, make sure you have a discussion with each senior manager (in the risk assessment meeting mentioned above is a good opportunity to talk to multiple managers at once) so that they understand not only why you are restricting their access, but how to recognize when they are being scammed. They will also receive more scammer emails on their personal devices as well, so they should appreciate your efforts to protect them.

Start with the highest risk items on your list and detail out the ways that someone could compromise that data. Then detail out the ways someone could expose that data, accidentally or on purpose. For example, someone may send payroll information in a plain text email because they don't realize that it could get intercepted.

As mentioned above, working hand in hand with your security professionals is pretty much a must throughout this process, but here is where it gets critical. In addition, subject matter experts are going to make this part of the process worlds easier on you. You need to have multiple options for protection, especially when budgets are tight. And you need to have support for when it comes time to implement and maintain your solutions.

Is that all? Am I done?

Unfortunately – you know the answer to this one – no. This is an ongoing process. Companies grow organically, and budgets and strategies constrain spending while sales and development call for creative solutions – at the end of the day, employees have to deliver on goals and objectives. However, once you have gone through this process once, you not only have a foundation to build on, you also have a good idea of what works and what doesn't.

The time to fit the whole process into a busy schedule is the biggest hurdle to getting started. Sometimes, if you just get that foundation started, you can find the time to dedicate to it each quarter or each year. If you need help getting started, Cornerstone has some excellent assessment tools and recommendations. And if it is just a question of time, we are here to help you get a good foundation going for you to build upon.

Need Assistance? Contact Us today:

Amy McNeeley: Amy@hmscs.com
Kathy Mortensen: Kathy@hmscs.com
Stuart Siegel: Stuart@hmscs.com
Karen Chamberlain: Karen@hmscs.com

Be the first to know when we publish a new whitepaper! Follow us online: