Sentinel IPS

Local Government:
Battling 6 Security Misconceptions

24/7 monitoring & one-of-a-kind Network Cloaking technology.
The Sentinel team relieves the burden of managing IPS and IDS once and for all.

✓ NETWORK KNOWLEDGE & PROTECTION ✓ TRUSTING YOUR NETWORK DATA ✓ THREAT INTELLIGENCE & PREPARATION

Here’s a pretty staggering number:

27,947,513

That’s the number of personal records exposed, according to the Identity Theft Resource Center, through the first half of 2015 because of government data breaches. While that number does include some pretty high profile federal breaches, it also includes many more at the local level that didn’t make national headlines.

What this highlights is the need for better security practices at all levels of government. But before the local governments can get serious about security, there are six misconceptions that need to be addressed.

6 Security Misconceptions

1. *All of our information is public, so a breach isn’t really that damaging.*
2. *I know exactly where my data is.*
3. *I can use security products straight from the shelf.*
4. *Last year’s training is enough to keep the network safe.*
5. *Other agencies are handling security for me.*
6. *Security is a shared responsibility.*

Misconception No. 1:

All of our information is public, so a breach isn't really that damaging.

While open records legislation has been wonderful for helping shine light into some areas of government that have been dark for too long, it's also created a bit of confusion for those tasked with controlling who can see what.

The confusion is somewhat understandable. The clerks working in some local government offices may see so many requests from activist groups or reporters or the public that they assume all information is public. All this paperwork is just a formality so keeping the data digitally secure isn't really necessary.

> *"The truth is, most information that's being held by local governments and agencies isn't inherently public."*

Some of it can be obtained through the proper channels, but that doesn't mean putting security in place to protect it isn't necessary.

How to battle this misconception:

This is a battle fought on two fronts. The first is employees who don't know any better. You have to educate them about what information is public, what is private, and when the court can order that information be turned over. While state and local governments do not have to adhere to federal Freedom of Information Act rules, all 50 states have adopted some type of open records law. So step one in fighting this misconception is making sure employees are familiar with the regulations that apply to them.

Use this Open Government Guide to determine what information is public in your state.

The second front in combatting this misconception is disorganized data. What do we mean by disorganized? Too many local governments can't tell HIPAA data, from criminal data, from Social Security numbers. This presents two problems. First is that without classifying data simply as either public or private, you are making the work of your local clerks twice as hard. And second, if you don't know what information is private, you don't know what information to protect. You don't know where to put your stoutest defenses and build your highest walls.

Data has to be managed in a whole different way.
It has to be segmented. It has to be segregated.
It has to be classified.

Misconception No. 2:

I know exactly where my data is.

There's one commonality among all the news stories about federal government data breaches. In each instance, officials knew exactly what kind of information was compromised. If those stories had been about local governments instead, the information wouldn't have been so detailed.

That's because at the federal level, network administrators usually know exactly what information is living where. If Server A was breached then that means names and addresses were compromised. Server C it's Social Security data.

At the local level, you may believe that you know where your data is, but you don't. Not specifically. With single servers handling multiple departments and applications, knowing where data is to the level of detail that the federal agencies have isn't possible. A single breach of a single server could mean that information from several departments has been compromised.

How to battle this misconception:

To some degree, the local officials aren't necessarily to blame. This is a misconception that can be blamed on dollars and cents. Buying a server for a single department or application is expensive, too expensive for many. Why buy four SQL servers when you only need one?

The solution: virtualization. Run virtual machines, splitting your apps that way, and do not let them cross. If you're using SQL servers, you are going to need to protect those databases. That means putting something on the wire that can recognize the difference between normal and abnormal calls and then something on the server that can segregate databases and permit only those with permission to access the tables.

Misconception No. 3:

I can use security products straight from the shelf.

Local governments have a problem with speed. They want to be able to move as fast as the private sector when it comes to security. The ideal scenario would go like this: Go to a tradeshow. Buy a device. Plug it in. Instant security.

Unfortunately, security doesn't work like that, not for local governments.

How to battle this misconception:

Every network is different. That's why, no matter the device, modifications are going to be required. Development is going to have to be done. The new device will have to be tuned to the network if it's going to achieve maximum effectiveness.

It's also critical that the equipment these organizations do buy be quality products. No going down the street to Joe's Firewall. They need to put in a real piece of equipment that does real work. The same is true for the IDS and IPS systems. Find a reputable vendor. Purchase quality products.

Another route to consider: outsourcing. Whether it's moving parts of your network to the cloud or using remotely managed devices, you can save money, time, and get top-level protection by looking to outside vendors to help you manage your security.

> *"It's critical that the equipment these organizations buy be quality products."*

Misconception No. 4:

Last year's training is enough to keep the network safe.

More and more, hackers are turning away from brute force attacks and malware as the means of getting into a network. Instead, they are counting on the naiveté, and some would say ignorance, of the typical employee. They are using social engineering schemes to trick these employees into providing them with legitimate ways to enter the network.

It's OK, though, because the training that was held a year or two ago covered all of those tricks. The network is protected. Well, if your company never hired another employee after that training, and if hackers weren't constantly evolving their methods, then that would be true.

How to battle this misconception:

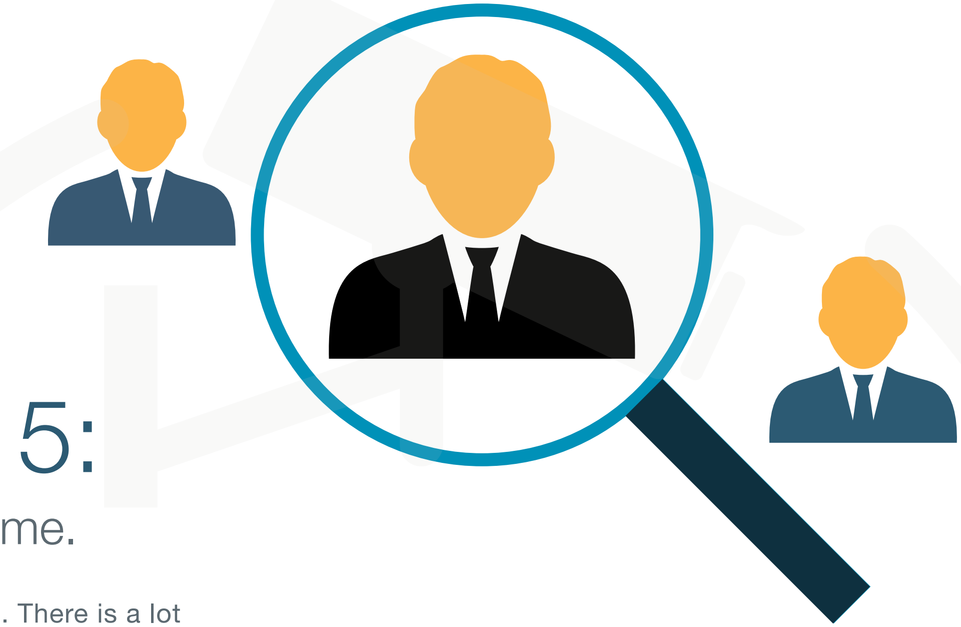
This one is probably obvious: more frequent training. Unfortunately, the execution of that training often falls to someone in the IT department, and training and educating aren't really in the skillsets of many in IT. With that in mind, here are some tips for effective training.

Use Simplified Language
IT speak can seem like a foreign language to anyone without training in the field. Speaking on a level that employees can fully comprehend is essential. Doing so will result in fewer of your employees being confused and unsure about what they're learning.

Encourage questions
The only way to know if what's being conveyed is being understood is by encouraging questions. Stop and ask specific individuals questions regarding the content in order to ensure that everyone is on the same page.

Regular education and testing
Hackers are continually trying new methods for getting into a network. Keeping employees up to date on these methods is critical. The easiest way to do that is with a regular newsletter that addresses new or recurring threats.

As the saying goes, a chain is only as strong as its weakest link. The only way you'll know where those links are is by randomly testing employees on social engineering tactics.



Misconception No. 5:

Other agencies are handling security for me.

This is a common misconception that is also a bit understandable. There is a lot of local data that state and federal agencies need access to. To get access to that data, those agencies are granted permissions on the local networks. The thought, then, is that since these larger agencies have access to portions of data then they are keeping an eye on its security. That's wrong. Here's an example.

Criminal data is regulated by the FBI. It regulates who can and can't have access to that data. But here's the problem. The FBI, just like other state and federal agencies, are only concerned with their processes. The feds don't care which database officers or agents look at as long as the person looking is a legitimate law enforcement officer and currently working for a local government. They are doing nothing to ensure overall security of the data. That is still the responsibility of the local government. But without anyone on staff thinking about security, these organizations are blind to their own security holes, and they won't know where their weaknesses are until they've been breached and something fails.

Misconception No. 6:

Security is a shared responsibility.

While every network is unique, there are two things that are common to almost all local government data centers: They have small budgets and small staffs, including some counties that are running with entire departments made up of one person.

Often, it's teams of two, three, four people that are responsible for not only maintaining the network, but also maintaining end point devices and taking help desk calls. They are sharing the responsibility for all IT projects, including security.

The problem is that when it's everyone's job to monitor the network's security, chances are no one is actually doing it because they assume "well, someone else has taken care of that." Security isn't something that can be done by committee. It requires dedication and focus.

How to battle these misconceptions:

Each of these misconceptions has the same solution: hiring someone who knows and can concentrate on security. The argument against this is obvious. It's not in the budget. The reality is you can't afford for it not to be.

The cost of even a single breach can be staggering. Today, the average server rebuild costs about $60,000 per server. If you get hacked, the chances are high that you will have to rebuild the server. It's almost an automatic $60,000 spent. And that's only to rebuild the server. That doesn't include any remediation costs that may come with a data breach, like paying for credit monitoring for anyone who may have been affected.

Without someone in place who knows security, you're betting that you're not going to be hacked, so you're not going to have to spend that $60,000. But a good risk manager would spend $60,000 up front to protect the server, because if you are hacked you're going to end up spending the $60,000 one way or the other. It's just a matter of when, how, and what other costs are going to be associated with it.

Identifying Candidates for Hire:

So, if hiring a security professional isn't a luxury but a necessity, how do you identify the right candidates?

Certified vs. Not Certified

The first decision you'll have to make, after deciding to hire a dedicated security professional, is what weight will you give certifications? There are a number of different exams out there that are conducted by numerous security organizations. Successfully passing these exams — including the CISSP, GSEC, and CISM — requires dedicating both time and money to the process.

However, earning a certification doesn't necessarily reflect on someone's ability to perform well. While they are valuable from an educational perspective and making the effort to earn one (or more) certainly shows initiative, proving experience through a technical interview or demonstration of skills is just as important. These certification exams don't always test for some of the more intrinsic character traits that make for an individual best suited to become a network security professional. Here are two we think everyone needs to have.

Detailed

One of the more innate abilities of good security experts is that they are excessively detailed and conscientious of their work. Reading a system log is difficult for most people, and you're not meant to speed-read every line. If you get into the habit of just cruising along and scanning a system log, it's easy to miss a detrimental action and write it off as a normal operation. A great security expert is able to not only understand the information and what it means, but is also able to focus while reading each line individually.

Independent

A good security team member also has the ability to work independently. He or she isn't thrown off by the need for a flexible schedule, realizing that network security isn't merely a 9-to-5 kind of job. The people trying to breach your network's security protocols don't only operate during normal working hours, so neither should your security team. Members should be able to work whenever they're needed, and they should be able to decipher a problem and come up with a solution without having their hand held by a supervisor.

The role of being a security expert requires more than just a few certifications and a little training. A proper security expert isn't in the position only for the title, because for them the trade is a state of mind. These are the people who like to understand everything about the way a system works and actively pursue these interests outside of a working environment. These are the types you want on your security team.

Conclusion

Hackers are getting more sophisticated every day, every hour. They are developing new methods and finding new vulnerabilities. They are trying new social engineering tactics. They also know what companies and organizations are the most vulnerable. They know the groups that have the biggest holes in their security and, therefore, are leaving them the easiest way in. All too often those businesses or organizations are smaller, like local governments.

That's why it's critical that these misconceptions about security be corrected.