CHAPTER 22

EMPLOYEE MONITORING

BY SEAN ROBERTSON

When the discussion of monitoring or limiting the computer-related activity of employees comes up with my clients, it's not unusual for them to say things to me like, "My employees are good people."… "No need for 'secret squirrel' here."… and, "My employees are my friends and they would never hurt me." I've heard these statements hundreds of times from small business owners and it can sometimes be a difficult conversation. The unfortunate thing is that some employers don't heed my advice to put proper monitoring measures in place until I get that "second" call to discuss the cleanup and aftermath of an employee (or partner) problem that caused a significant issue.

Recently, I worked with a small multi-national company with three offices in three countries with approximately 35 office employees collectively. This company was growing fast and was using acquisition as a means to fuel their growth. After one acquisition, they hired the previous business owner to be the General Manager of the US-based operation.

The integration went very smoothly from an operations perspective, but there were a few challenges that almost lead to the bankruptcy of this business. In the excitement of the new acquisition, no one looked

at the technology being used by the acquired company other than the accounting system.

One Friday afternoon, which often seems to be the day problems are discovered, one of my senior technicians received a phone call from the client. The phone call started with, "I'm so glad you're available. We haven't been able to access any of our data for three days. I've got to get payroll done and I've got to invoice my clients. Can you help?"

After a small bit of investigating, the problem was becoming more defined. Whenever a file was opened, it couldn't be read. Microsoft Office and every other piece of software said the files were not readable. The files could be seen, they weren't gone, but they just couldn't be opened. Two of my senior technicians spent the next 72 hours trying desperately to understand what was wrong.

The hardware passed all of our diagnostics, but we still couldn't open the documents. The data showed no signs of corruption, but couldn't be read. At first, this was happening on just one server, and then it spread. At the end of the third day of attempted recovery, the data on the second server now had the same problem. And, because of the way the client elected to perform backups, the backup data had the same problem. At this point, there was only one known useable copy of this client's data and it was seven months old.

Not having this data would lead to significant financial issues as well as service delivery issues for this business. An additional concern in this situation was that the client was also storing someone else's data 'as a favor' and that data was also not usable.

Overnight on Monday, almost every computer in the office was scanned for virus and malware. Unfortunately, every computer came back positive with various forms of malware. However, none of the malware seemed to be related to the problem. There was, however, one computer that we were unable to scan that night because it was not made available to us. It was the computer used by the former owner and now General Manager. He had "forgotten" to give us access.

He had also "forgotten" to tell us that on the previous Monday, his computer had become infected with Cryptolocker, a nasty piece of malware which holds your data ransom. It does this by encrypting any

and all data it can find and then demands a payment to have it decrypted. In fact, one version of this doesn't even make the demand, it simply waits for users to search the Internet for a solution and then sells decryption software through a legitimate-looking website.

There is of course more to the story. It was discovered that the General Manager had picked up the virus while surfing inappropriate sites while at work. After realizing he was responsible for allowing the entrance of a virus, he was embarrassed and spent a day trying to solve the problem himself. He then called in a local technician to solve the problem. The local technician wasn't very experienced and removed the virus without informing anyone of potential consequences.

All of this could have been prevented if the proper monitoring protocols were in place. If for some reason the website was not blocked, the monitoring system's antivirus system would have stopped the delivery of the virus. The crisis would have been averted and money would have been saved.

The client eventually spent over $35,000 and fifteen days of downtime, but we were not able to recover all of their data. Instead we had to use a backup from their most recent server upgrade that was seven months old. Fortunately, this company had the resources to recover their data. However, not every company is so fortunate, and the consequences of losing every piece of data you have can be dire – to say the least.

There are many things that the company involved in this story could have and should have done differently. Backups weren't performed properly, desktop and gateway antivirus wasn't in place, and all users had "super user" access. These are all very significant problems. But the crux of this particular problem stemmed from the fact that there was no employee monitoring system in place.

When most people think employee monitoring, they think about stopping employees from visiting non-work related sites. This is of course with good reason. Recent surveys indicate that 39% of employees spend between 1 and 10 hours per week surfing non-work related web sites.

However, there is another significant risk of not having an employee monitoring system. It's a legal and a financial risk. If you permit (or do not stop) employees from visiting objectionable websites, you are

placing your company in a place of vulnerability in many ways. Imagine an employee viewing pornographic material on their work computer. Now picture another employee walking up behind that employee and seeing the pornographic material on the screen. You are now potentially on the hook for a harassment lawsuit or some other type of litigation.

Related to this topic, we were called to a business to investigate a problem of a very slow network. As we were telling the employees what we were going to investigate, one person appeared very, very concerned and asked about their right to privacy. Through our investigation, we found that not only was that employee keeping child pornography on his company-issued notebook, he was distributing it to other people on the Internet through the corporate network. In this particular case, the authorities seized that employee's company-issued notebook and another company computer and kept them for six months. Unfortunately, the business was not able to gain access to any of the company-related files on those devices because it became evidence in a police investigation. Think of the ramifications of this incident. The company lost a computer and notebook, experienced work disruption because of the investigation and had to pay for IT services to discover a problem. Add to this the potential negative press a situation like this can bring to the company, even though it was an employee of the company and not the company itself being targeted in the investigation.

Recovering employee time and preventing lawsuits is obviously appealing and the savings can be significant. But really, those savings pale in comparison to the cost of losing your business. Both of the examples above could have been avoided with an employee monitoring system.

Many times we've gone into companies to do an audit and have found 10 or 15 people who are no longer employees but still have access to the network and have recent logins recorded. This happens all the time. While I consider this to be the utmost negligence in IT security, it's not a rare incident.

Small businesses are preyed upon by the bad guys because the small business owner typically has limited resources to protect their data. People assume that bad guys are stupid, but they're not. You can actually hire crime as a service today. You can go to an underground bazaar and

subscribe to almost anything you want. You can hire a hit man, buy drugs, or buy a block of credit card numbers. The selection of crime activity is almost limitless. This is not an exaggeration that is espoused by the Information Technology community to sell their services. There is a very real threat that exists to individuals as well as to business interests. Unfortunately, many times individuals and businesses don't fully understand this risk until tragedy strikes them.

As a business owner or leader, it is your responsibility to take a proactive approach to put into place monitoring resources that will protect your business concerns and your employees while they are conducting work on your behalf. Below are some suggested steps you can take to protect your business and improve employee productivity:

1. CREATE AN ACCEPTABLE USE POLICY

This policy should be in writing and should define what employees are allowed and not allowed to do with company resources such as smart phones, computers, tablets and Internet access while in the office or out of the office. A qualified IT provider can help you develop your policy. But, here are some things to consider as you develop this policy:

- What type of web sites are employees allowed to visit?
- Can they download movies or music?
- Are they allowed to have non-work material on their computers?
- Are their children allowed to surf the web or watch movies on the device?
- Are they allowed to install software on their own or do they require permission?
- What is being monitored and why?
- What can the employee expect for privacy?
- Will you monitor email?
- How will you monitor non-work email addresses they access via company assets?
- Tell them they must not do anything illegal using any work-related devices or equipment.

2. BE UPFRONT WITH YOUR EMPLOYEES

There is no reason to hide the fact that you monitor and control employee use of company resources. Make sure your Acceptable Use Policy is in writing and that every employee has a copy. It may be a good idea to include your Acceptable Use Policy in your Employee Handbook. Your policy should be discussed with existing employees and should be part of your new employee orientation. Choose the method of communication that works best for you, but be sure to let them know you are monitoring, why you are monitoring and what you are monitoring.

Often small business owners don't want their employees to feel like "Big Brother" is watching over them. However, that sometimes leads to financial loss. It is best to monitor and prevent a problem rather than clean up the chaos caused by a problem. Tell people what you are doing, how you are doing it, and how you will use the information you collect. Let them know that you are not necessarily monitoring any one person specifically, although you can and sometimes may have to monitor specific individuals if there are reasonable suspicions. But, more importantly, let them know that you are looking for patterns to protect the business. You will find that most people will readily adapt to your established policies and accept it as a condition of employment.

3. START FILTERING AND MONITORING

Your main goal is to protect your business from what employees intentionally or unintentionally may do to harm your company. At the perimeter you can set up a Unified Threat Management (UTM) system that looks at all the information that comes into and goes out of the network. UTM can monitor and dictate what websites can be looked at by employees and blocks viruses and other malicious software before it gets to your network. You want to protect your business from sites that can potentially bring harm to your internal systems. This will prevent employees from accessing sites that may be full of malware or are inappropriate as determined by your corporate protocol. This is the first level of monitoring that I recommend businesses employ.

You will also want to make sure you filter all outbound and inbound emails. Company secrets can disappear via outbound email and spam and viruses can be introduced via incoming email. If an employee

inadvertently becomes a spammer, your filter will catch it and protect your company's Internet reputation.

The next step would be to look at desktop and laptop monitoring and filtering. You will need to decide if you are trying to protect, monitor or both. If needed, you can conduct specific device monitoring to determine what applications a particular employee had open, when they were opened and whether or not that employee was actually working. Specific device monitoring can record every keystroke made by the employee if that becomes necessary.

When you have mobile devices that leave the safety of the inter-office network the mobile devices can be misused and can become vulnerable to acquiring a malicious virus. However, device monitoring can mitigate that risk by applying the same filters on any mobile device. Basically, the same controls that are in place for your network can also be placed on all your mobile devices. It's a little tougher to monitor smart phones as there are very few tools to help manage those devices. There are some, but they aren't very robust.

Filtering and monitoring not only keeps the bad guys from getting in, but it also keeps protected information from getting out. You can put filters on network and mobile devices that say, for example, "Make sure that nothing containing a social security number ever gets sent. If it is included in an email, forward a copy of the email to this monitoring station because it violates our established terms of usage." While you can't look for specific documents, you can look for key words or key indicators that indicate something wrong may be happening.

If you are concerned about the protection of your Intellectual Property or trade secrets, there is software that can be installed that will prevent the unauthorized usage of any USB drives in your computers. If USB drives are used, they must be a USB drive that is issued by the company with a certain identification number and specific encryption. When it is plugged in, the computer will recognize it as an authorized USB and will allow information to be transferred from the device to the USB or from the USB to the device. This is not as much a monitoring activity as it is a prevention activity, but it is a methodology that can certainly save a business under certain circumstances.

4. REVIEW AND UTILIZE THE REPORTS

There will be numerous reports you will want to monitor because they have the ability to save you a lot of time, money and overall headaches. Essentially you want to look at the type of traffic coming into your network and going out from your network to see if it makes sense. It's not usually about finding out that a specific employee has done something wrong, although it could certainly lead to that, but it's about being alerted to potential problems because of idiosyncrasies in the data.

When monitoring reports, you will want to be looking for the exceptions and things outside your normal activity. For example, let's say you had 7,000 visits to sites that are trying to download malware to your network. You may recognize that as unusual because you usually get just one or two a week. That tells you there is a problem. Increased attempts to reach a site that has malware on it probably means one of your machines is infected with something and it's trying to spread or call home for instructions.

Your email reports will also give you important information. For example, if your company normally sends around 1,000 emails per week and this week you see there were 50,000 outbound emails; that may be indicative of a problem. Increased mail activity may be an indication that there is a spammer trying to send email through your network.

Make sure you are using the report data appropriately and efficiently. If there is an indication of a problem, have the problem researched further and resolve the issue before it becomes an even greater problem. If your investigation leads you to a specific employee, be committed to appropriately discuss with the employee questionable behavior or activity. There is little point in identifying a problem if you are not committed to resolving the problem to protect your business.

5. TAKE A PROACTIVE APPROACH TO EMPLOYEE MONITORING

If you have a business, you **MUST** put monitoring safeguards in place. If you don't, it is an indication of the value or lack of value you place on your work. Sometimes business owners will use cost as a reason to not have appropriate monitoring in place. It may surprise you to know that monitoring can be done at a very reasonable price. In fact, the price of not monitoring is too high to not have the proper monitoring practices in place.

About Sean

Sean Robertson has been working with business technology for more than thirty years. When he was only sixteen years old, while still attending high school, he co-founded Universal Programming in Halifax, Nova Scotia. After working his way through school developing payroll and manufacturing systems, he accepted his first "real job" supporting and installing accounting, point of sale and front desk systems throughout Atlantic Canada. After settling in Moncton, New Brunswick, Sean accepted a leadership role with General Electric Appliances Canada and was able to further round out his experience by accepting leadership roles in Technology, Customer Service, Logistics and becoming certified as a Six Sigma Green Belt.

After several years with GE, Sean accepted a role with an international manufacturing company leading the Customer Service, Manufacturing Operations and Technology teams as Vice President Operations and Chief Information Officer.

In 2007, Sean recognized an opportunity to bring enterprise level technology management to small and medium business and founded Strategic Technology Associates (STAI).

Spending so many years leading customer service and technology teams at an Executive level provided a strong foundation for building a client-focused, results-oriented information technology services company. Sean is often heard saying how proud he is that his first customer is still a valued customer.

Strategic Technology Associates operates throughout Atlantic Canada, using a different strategy than most other technology service providers. The business model used by STAI doesn't permit profit from client computer problems. Instead; networks, desktops and servers are managed proactively to minimize downtime and save money for clients.

You can find Sean at:
sean@stai.ca
www.twitter.com/StrategicTech
www.facebook.com/getstrategic