

HOW INSIDERS STEAL FROM YOU

The Solution that Finds and Stops Them

Introduction

Employee computer usage comes with risks that frequently go unrecognised or are glossed over with a “we have something to deal with them” when in fact solutions in place are either inadequate or are simply not there. Here’s an example of what I mean:

I spoke with Sam, the head of IT, about how he secures critical information from being sent without authorisation. I asked specifically, “How do you know what information is leaving the company by flash drives or email? How do you stop what should not be going out?” And a growing concern with rapidly increasing worker mobility, “How do you ensure security when laptops and smartphones are off network? Say in an aircraft at 30,000 feet?”

Sam said that he locks down USB ports, although not for everyone, and he can review email on the Exchange Server. No answer for the aircraft.

Locking down USB ports doesn’t extend to everyone so that’s an obvious security hole. Checking email logs is time consuming and in reality doesn’t happen in the busy life of an IT admin. By the time you realise your competitor has your latest “sealed” bid it’s too late, the cow has been milked. Grrr!

This paper talks about three things: 1) threats you don’t know about or are being dealt with inadequately; 2) how to find them; 3) and most importantly, how to stop them.

Insider Threat Defined

There are numerous definitions of Insider Threat Prevention. I’ll define what I mean by them so we’re on the same page.

The word **threat** sounds ominous, but it goes beyond malicious activity (such as stealing the customer database) to include operational deficiencies (such as mistakenly sending financial projections to the wrong person or even to someone outside the company).

Insiders have access to resources. No need to break through a firewall; they’re already there. Needless to say, these can be far more damaging than external threats.

Prevention encompasses identifying risks, using the archived information to improve operations or provide evidence, and stop the threat from happening.

There are numerous solutions from a variety of vendors. That requires engaging multiple vendors, assessing solutions, then learning, implementing and providing ongoing support for the various applications.

If you're concerned about the resources to manage an assortment of applications, an integrated security platform may be the solution you are looking for.

This paper, after identifying the risks, details vendors and their technologies that deal with them. Lastly, it proposes an integrated solution that eliminates the complexity, resources and time required of dealing with numerous applications.

If you're concerned about the resources to manage an assortment of applications, an integrated security platform may be the solution you are looking for.

The Threats and their Solution

These scenarios illustrate types of risk and how to deal with them. They are unfortunately common enough. The good news is that they can all be either prevented or at a minimum documented with detailed evidence. These all happened.

Loss of information

- Justin plans to put computer code on a flash drive while on vacation and off-network. He figures the company will not know or be able to stop it.

The solution: Data Loss Prevention policies that work on the end point, that do not require a laptop to be connected to the company network.

- Oliver uses Hotmail to offer marketing plans to a competitor he plans to work for. He subtly composes the message so his intent would be hidden should the email be read by his employer. He deletes wording that might be a tip-off, but what remains is enough to arouse suspicion.

The solution: Fortunately, the security officer had installed monitoring software, which included a keylogger that in addition to recording formatted data also records function keys, such as the backspace, so deleted words were now visible. They now knew what Oliver intended and confronted him – and his prospective employer. End of problem.

- Jeanne and Raymond both report their laptops stolen. Each has crucial information on it. All company data is encrypted, so supervisors expect the information to be secure. Nonetheless, regulators require reporting what information is on the laptops.

So Jeanne and Raymond and their supervisors huddle in the conference room to figure out what exactly is on those laptops. Memory being a poor substitute for certainty, the conclusion is anything but sure. And it turns out that Raymond had put files on his laptop against company policy and he wasn't going to own up to it.

After several days a competitor begins soliciting their customer base. With further investigation it turns out Jeanne was in the habit of putting a sticky note on the bottom of the laptop with the encryption password because passwords being complicated and replaced regularly, she couldn't remember them. Result: Richer thief. ☹

The solution: Have a laptop tracker installed that geographically locates the machine (like TRACKER (www.tracker.co.uk for cars). But recovery of the laptop is not foremost; it's the ability to know what information is on the laptop, retrieve it, and most importantly, delete the files – and not having to report data loss to regulatory authorities such as the Information

Commissioner's Office (ICO). A bonus is recording the thief's activity, usually discovering his identity, which often results in the return of the laptop.

This happened to a major bank. After recognising the security hole, with hindsight being better than no sight, the bank installed laptop tracking software on all its laptops.

- Wendy is preparing to leave the company and takes a picture of a technical drawing on her smartphone to share with her new employer.

The solution: The use of mobile devices is rapidly becoming prevalent. What has not kept pace is the awareness of this security gap. It is essential to know how smartphones are used, what information is being sent by them. Smartphone surveillance technology enables the recording of email, text messages, photos, call logs, and GPS monitoring. It can also send an alert when particular words are used.

Know what information is on the laptop, retrieve it... delete the files – and not have to report data loss to regulatory authorities.

Productivity loss

- Jessica is deputy head at a Higher Education college. She's taking an advanced degree herself. Good for her. However, it turns out she is spending four hours a day on assignments during office hours! Not good.

The solution: The college installed monitoring software because they lacked the means to know if their Acceptable Use Policy was being complied with, in particular the amount of time spent on personal things. They easily, and to their surprise, discovered Jessica's abuse. But what they also learned was that Grace, her assistant, was 99% on-task. What did they do? Fired the one and promoted the other. Sounds like justice to me.

- Dan, IT Manager in this healthcare company of 100, knew there was substantial time spent on personal activity.

The solution: Dan installed monitoring and for two weeks gathered data for a baseline of activity against which to compare after monitoring was announced. Turns out about 30% of the day was personal activity! He wasn't interested in catching anyone, just getting people on-task. So he not only announced monitoring, but also showed a few anonymous examples. The result was spectacular. Immediately productivity skyrocketed. In fact, over the year ten employees left for various reasons and he didn't have to replace them. Around £200,000 saved annually. Brilliant!

Immediately productivity skyrocketed. In fact, over the year ten employees left for various reasons and he didn't have to replace them. Around £200,000 saved annually.

Regulatory compliance error

- This company to meet financial and PCI compliance requirements installed a centralised Customer Relationship Management database so information, such as identity and financial information, was no longer on local machines, particularly laptops in the field. But how to know if everyone had deleted their local store of customer information?

The solution: They installed a solution that searched files on *every* computer for customer records. It turns out that a good number of sales people were keeping this information locally. And what's more they updated the local cache rather than the central database so the true state of customer activity was unknown to managers. Through the software they were able to remotely delete these files, even on off-network laptops. What's more it alerts management if customer information is put back on a computer.

- Ian knew that company policy prohibited the use of webmail. But the mail server was down and Ian wanted to get an important customer quote out so he used his Gmail account. Oops!

The solution: The Company uses Data Loss Prevention (DLP) software that checks each email. It flagged customer information going to a webmail account and kept it from going out. The way things ought to be.

Litigation Risk

- A law firm fired Bill because he was spending an awful lot of time Instant Messaging with his girlfriend, using proxy servers to get around the web filter – you name it, he did it. Next thing the company knows the employee has the gall to apply for unemployment claiming he was unjustly terminated. Now what?

The solution: Fortunately, the Company had installed monitoring software as part of its efforts to increase productivity. And it worked very well by the way, reducing an average of one hour/day off-task to 20 minutes – quite acceptable; the company knew in this digital age that employees had personal lives that needed attending to during the work day.

For Bill they had the evidence, so they contested the claim and showed it at the hearing. Claim denied. They have done this on several occasions now and have saved quite a bit in unjustified claims against the Company.

Unintended threats

Threats to an organization go beyond malicious intent. Often enough they are unintended, but damage results nonetheless. Here are some examples. They can all be prevented.

- “Reply All” is selected to an email with a confidential customer list. Unbeknown to the well intentioned sender is that one of the email addresses is external to the company. Oops! Similarly, as an email address is typed it is auto-populated – to the wrong person.

The solution: DLP policy that prevents sensitive information from leaving the company, but that also presents senior level people with an ‘override’ function.

- An employee is off network. The web filter requires access to the server, so it is unable to prevent him from visiting a known website that installs malware - which now enters the network when the employee connects to it.

The solution: Web filtering software that works on the endpoint, that does not require access to the network bound web filter server.

- A financial company is regulated in regard to providing investment information. A big *no-no* is guaranteeing a return on investment. A broker gets carried away and emails a customer about a stupendous investment - and uses the word *guarantee*. Uh-oh!

The solution: DLP software triggered by the alert word “guarantee”, thus preventing the email from going out. It also advises the employee why it was blocked so he learns from the error, and logs the activity for a supervisor to review.

Available Solutions

Here is information on technologies that address each area of Insider Threat Prevention. I compare some of them with Snapguard 2.0, the product we developed. I feel it’s objective and worth your time.

Monitoring

Monitoring records activities so they are documented and can be reviewed to find security loopholes. And there are positive uses, such as improving operational practices and quality control - and a whole lot more. But that’s outside the scope of this paper.

Now if you’re concerned about privacy issues, you can protect information with only Data Loss Prevention; you do not need monitoring. But us humans not being perfect, what monitoring does is ensure you have the policies set up correctly. (We have a paper on privacy and how to introduce monitoring: *Employee Monitoring Made Easy: How to have Staff Embrace Computer Monitoring*. [Click here](#) and request a copy.)

Data Loss Prevention (DLP)

Symantec DLP and McAfee DLP are premiere solutions. They are designed for the enterprise with high costs for the software and significant cost for hardware. They require substantial staff resources to configure policies and maintain them. This makes this solution practical for very large organisations.

[Symantec DLP](#)

[McAfee DLP](#)

By contrast, Snapguard 2.0 Data Loss Prevention is not as robust, but it does the job quite adequately for the vast majority of companies - and much more simply. Its policy creation for example is much easier.

Working on the endpoint it does not consume network/server resources to process policies. And very importantly: it works when a computer is off network, such as an employee on a cruise liner who attempts to send a customer list to his USB drive. With server based DLP solutions, if the computer is off network or the server is down then the network loses its protection. Processing at the endpoint eliminates this risk.

(Snapguard 2.0) works when a computer is off network, such as an employee on a cruise liner who attempts to send a customer list to his USB drive.

USB Port Blocking

Cryptzone's Secured eDevice includes USB protection. It turns USB ports either on or off; it does not scan content against policies. <http://www.cryptzone.com/products/edevice>.

Port blocking is included with Snapguard 2.0 DLP.

Laptop Tracking

Absolute Software is Lojack for laptops. Works quite well. It does require a police report before the process of locating the laptop can begin. Filing the report and Absolute Software doing the locating extends the time for action to be taken.

<http://www.absolute.com/en/lojackforlaptops/features.aspx>

By contrast, Snapguard 2.0 Laptop Tracker requires no police reports; its functionality is available immediately upon report of a lost or stolen laptop. It includes the ability to see what files are on the laptop, retrieve and/or delete them. It can also block programs from running, effectively making the laptop unusable. Furthermore, it monitors the activity of the thief so it is fairly easy to identify him as he logs on to his Facebook account, sends email, etc.

(Snapguard 2.0 can) see what files are on the laptop, retrieve and/or delete them....It monitors the activity of the thief so it is fairly easy to identify him...

Mobile Devices

Mobile devices are an increasingly important focus for security, but one I feel that is not acknowledged as it should be as a source of security breaches. A few high profile cases will make this known.

At a minimum, email and text messages should be recorded.

Web Filtering

Server based solutions are in wide use, such as WebSense (<http://www.websense.com>). They are dedicated, robust solutions.

By contrast, Snapguard 2.0 Web Filtering has features not available in server based web filters. Working on the endpoint enables filtering to continue working when a computer is off-network, such as a laptop away from the office. Additionally, if a web server fails all computers lose Internet

access. But Snapguard 2.0 being only on the end point, failure of any single point does not affect anyone else's Internet access.

The additions of triggered screenshots provide a snapshot or video recording of targeted activity. This could include for example sending Gmail so you have a visual record of composing and sending it.

Another feature not usually found in filtering programs is the ability to see what programs are being used and how actively. You can also block them or allow use according to a schedule.

Lastly, Cloud delivery does not require local installation, so you will save on computer hardware and maintenance resources. And it makes installation simple. (OnPremise installation is also available.)

Conclusion

We've viewed the treats, malicious or inadvertent, shown how monitoring documents them, and provides solutions to prevent them.

There are a number of good solutions out there. Keep in mind that you'll have to work with several vendors and spend time evaluating each product, then implementing and supporting it. That's why an integrated solution should be on your list to consider.

Whether or not you use several vendor products or an integrated platform to comprehensively guard against Insider Threat, the ideal is to put in place the following solutions:

- Data Loss Prevention (DLP)
- Computer Monitoring
- Laptop Tracking
- Mobile Device Monitoring
- Web Filtering

These solutions pay for themselves just in increased productivity – often many times over – without even considering what it would cost if the crown jewels were delivered up to your competitor.

Now for an unashamed commercial plug

There are vendors that integrate some of the above solutions. I have not found any that include all five cornerstones of Insider Threat Prevention. This is why Snapguard developed its integrated platform.

In regard to budgeting, you don't have to buy the whole package; choose among the modules. For example:

A company purchased 250 licenses of Snapguard 2.0 Filtering (this is extremely well priced compared with traditional server based solutions) and budgeted for the monitoring module in the following year.

To assist with budgeting, licensing is flexible. You can take a monthly subscription so it becomes an operating expense rather than capital budget item. And begin with a single department and expand from there.

Let me repeat a feature of unique value to Snapguard 2.0: it is deployed at the end point. This means you can record activity and enforce policy on every computer, even those that never connect to the network. The other standout feature is its two options for delivery that set it apart: through the Cloud or OnPremise as a configured appliance.

Snapguard 2.0...is deployed at the end point. This means you can record activity and enforce policy on every computer, even those that never connect to the network.

What's next?

Think seriously about protecting your company's assets – and improve productivity along the way. If you're an IT manager the CEO will appreciate your initiative and effort. If you're the CEO, then the Board of Directors will have one more reason to know they have the right person on board.

I'm sure you're like me in that you feel good when you've shared ideas that help someone. I love telling others how to protect their organisations. The success stories I hear keep me going. What I don't like to hear are the accounts of buying insurance after the house has burnt. Fire prevention is so much better than unreeling hoses. Spend your time running your business, not being a fireman. (OK, maybe as a kid you wanted to wear the helmet.)

Time is not on your side. I urge you to take action, do *something* now to protect yourself. Begin reviewing the various solutions and how they address your concerns. You have a number of places to begin.

[Click here](#) if you'd like our help sorting it all out. Contact us for a free productivity and security consultation. We'll give you our best brain. (Not quite Einstein, but we try.) We'll point you in the right direction and tell you like it is about what make sense for your organisation.

Good success and happy trails to you.

Contact Information:

HelpMe@SnapguardCorp.com

UK: +44 (0) 845 643 6881

Ireland: +353 (1)640 182

USA: +1 (407) 926 4139

www.SnapguardCorp.com