Why Data Loss Prevention Solutions Are Failing To Stop Insider Threat Attacks

On the 25th of June, McAfee one of the biggest security software companies in the world filed a lawsuit against a number of the former employees, accusing them of stealing trade secret before starting new positions with Tanium (a competitor).

To carry out the alleged theft, the employees did not use the type of sophisticated technology that you might expect. Instead, according to the

lawsuit, confidential company information was moved to unauthorised USB devices, as well through private email addresses.

Ironically, a company that professes to be the leader in security solutions around **Data Loss Prevention** suffered its fate.

Lets first identify Data Loss Prevention objectives. The role of DLP technology is to **identify, monitor and protect data in storage as well as in motion over the network**. DLP systems are used to enforce those policies to prevent unauthorised access or usage of confidential data. Data loss can occur due to intentional misuse, leakage, carelessness or theft.

The question then stands up as to why didn't McAfee utilise its software to protect its intellectual property?

- Is it because its DLP solution is ineffective? Or
- Is it because they trusted their people and decided not to use the software to protect their assets? Or
- Is it because it was misconfigured and didn't detect the data theft? Or
- Worse case, it just didn't catch the incident?

The Insider Threat Division of CERT published a number of key points when it comes to information theft:

1. Most insiders that steal information as they are leaving the organisation;
2. Around 75% of insiders that took information has authorised access to it;
3. It's tough to detect such theft as they are already have authorised access and usually steal it during business hours

But the question remains. Why do Data Loss Prevention (DLP) solutions are no longer effective?

Part of the challenge is that data has never been more portable. So taking it has never been easier. Sales lists, product specs, pricing information, payroll data and even contact lists are just a few examples of small but critically essential files that are simple to take. Employees can store hundreds of gigabytes on their mobile devices, put 1TB or more of data on removable media, or quickly transfer data to personal cloud storage services like Dropbox.

Not only is data moving around more, but so are employees. The median tenure of U.S. workers ages 25 to 34 is just 2.8 years. And as they move from company to company, they take data with them.

The second part is that implementing data loss prevention technologies is cumbersome to deploy and realising the full value is problematic (incomplete deployments is common). On top of it, DLP solutions require considerable maintenance, resources and endless fine-tuning.

However, the main challenge with DLP solutions is that it is trying to solve a technology problem, which isn't a technology problem. It's a "people" problem.

Data by itself does not walk out of the building. It requires the action of a person.

The question is why do people steal information? According to Insider Threat Division of CERT, majority of information theft is not for financial gain, but rather they take it with them as they leave the organisation or to take to a new job, give to a foreign country or start their own business.

There are two key variables in this equation.

A **cause and effect** relationship is when something happens that makes something else happen. In this example, data is being exfiltrated (effect) as a result of an action caused by someone (cause).

DLP solutions focus on the result (Effect). But such prevention technologies will never solve the real issue… which is "fixing" the real cause of the problem – "people" and their associated intentions… Why are they acting this way? How do we mitigate their behaviour? How do we deter and disrupt their behaviour from committing such malicious acts?

What Can You Do?

It is critically important that all levels of management and executive recognised and acknowledge the threat posed by their current and former employees, contractors and business partners to take appropriate steps to mitigate the associated risks.

To better protect your business from information theft, here are some best practices that I suggest you adopt:

- Identify your critical assets
- Periodically review and adjust your access controls for critical assets.
- Recognise efforts at concealment
    - Insiders exhibited an unusual degree of possessiveness on their equipment
    - Ability to detect illicit actions
- Have a process where employees can report suspicious behaviour
- Pay close attention around resignation.
    - The one month window or maybe more
    - Consider targeted employee monitoring
    - Establish consistent EXIT procedures
- Develop and enforce proper use of removable media
- Develop and enforce proper use of personal email
- Monitor for user, data and system anomaly behaviour
- Establish policies & procedures that your trusted business partners understand
- Develop an IP Agreement that new employees are employed
    - Ensure they have not brought any IP from the previous employer
    - Ensure any IP developed in house belongs to the employer

How Can We Help You?

Interested in identifying strategies in how your organisation can increase its effectiveness ability to prevent, detect, deter and respond to insider threats then get in touch with CommsNet Group or contact us +61 2 6282 5554 or feel free to fill out the form of the CommsNet Group website: https://commsnet.com.au/contact-us

Contact Us

For more information, you can also send them an email at: info@commsnet.com.au OR give us a call at: +61 26282-5554.