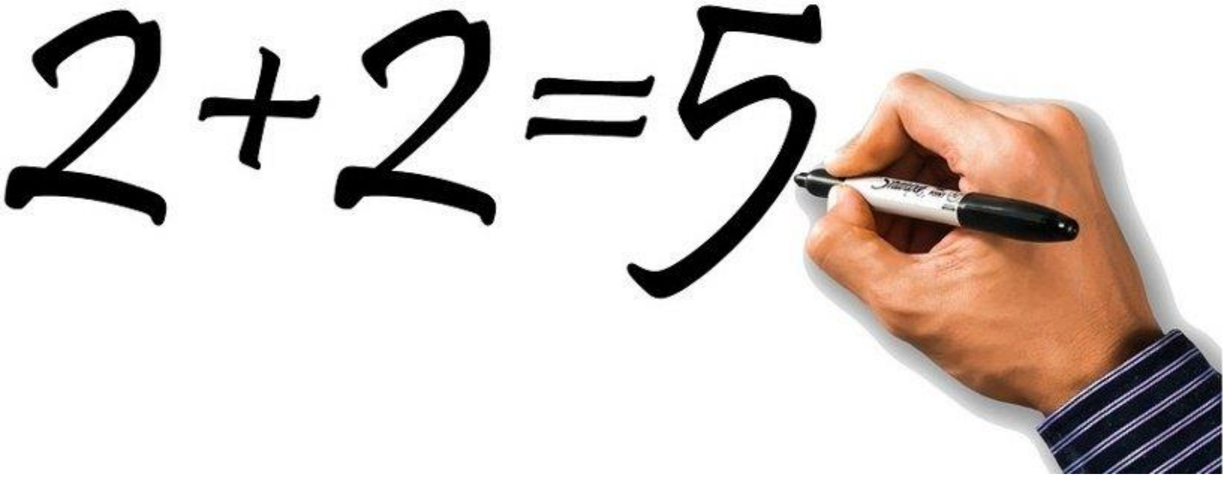
To Err is Human



"To Err is human, but to blame someone else is politics"

- Hubert H. Humphrey

The threat from accidental insiders is a reality across any organisation. Traditionally the emphasis has been placed on ensuring that an organisation was guarded against external threats, using permitter defences such as firewalls and layered security mechanisms. However, the current reality is that there is a far greater threat posed from those within the organisation. Industry reports and academic literature underline the fact that risk of accidental insider's compromise is potentially more pressing than that posed by outsiders.

Making mistakes and learning from them is a huge part of our lives. We never stop learning, even as adults. And we never stop making mistakes either. However, some mistakes can be costly. Error at the workplace can be disastrous and can cause damage worth millions to the business and potentially place people lives at risk.

Unfortunately, there is no such thing as a perfect human being. Part of our DNA is making mistakes. That's how we learn, grow and adapt. We learn from our experiences. And experiences are based on failures as well as success.

Prevalence of Employee Error in Data Breaches

A finding conducted by Gemalto in 2017 called Breach Level Index revealed that 76% of all the breaches occurred because of employee error. The worst part is that they could have been easily prevented.

No matter how good a business's security system is, it can all be brought down by a simple employee error. From weak or incorrect configuration setting, failure in following processes to accidentally posting sensitive information in the public domain can result in a major catastrophe.

Understanding the Intent

Internal breaches through employee error can also be further divided based on the intent behind the action. This intent can be grouped into the following different categories:

- **Intentional and Malicious** – These incidents are deliberate and are meant to cause harm to the business. They include actions such as theft of data and IP, conducting fraud by manipulating unauthorized systems, disabling critical service and much more.
- **Intentional but Non-Malicious** – These incidents arise from deliberate actions but there is no intent to cause harm. Non-malicious actions include downloading non-authorized software to circumventing organisation policies in order to "short-cut" a process.
- **Unintentional** – These are related to incidents that occur from mistakes in certain actions. These include saving a file in the wrong place, accidentally emailing someone, forgetting a detail or more.

Occurrence of Internal Breaches Based on Intent

Depending on the intent behind the incident, the figures for internal data breaches can be further divided into the following different numbers:

- 6.2% of internal data breaches were intentional and malicious.
- 9.1% of the internal data breaches were intentional and non-malicious.
- 84.7% of internal data breaches were caused unintentionally.

These figures highlight just how prevalent accidental internal breaches are and that there is a growing need to correct employee errors.

Total Number of Data Breaches Including Employee Error

Collectively, the number of data breaches is growing with each passing year. A report titled *'The Year of Internal Threats and Accidental Data Breaches*' by Gemalto highlighted that a total of 2,600,968,280data breaches occurred in 2017.

These data breaches were spread across different industries as shown below:

Industries	Records	Percentage
Other	1,356,031,744	52%
Government	465,014,660	18%
Technology	404,698,020	15%
Financial	235,563,765	9%
Entertainment	34,484,948	1%
Healthcare	33,717,772	1%
Education	33,400,663	1%
Social Media	19,202,738	<1%
Retail	13,961,106	<1%
Industrial	2,394,448	<1%
Professional	1,188,119	<1%
Hospitality	1,099,216	<1%
Insurance	135,359	<1%
Non-Profit	75,722	<1%

Out of this number, 76% of all the breaches (1,985,095,967) occurred because of employee error. Many businesses don't consider the internal risks they face which can lead to data breaches. Often, external sources are considered to be the bigger threats.

Since more focus is on these threats, businesses are often completely blindsided when an internal data breach happens. For many, recovery from a data breach can be very difficult.

Major Examples of Big Data Breaches Caused by Employee Error

The impact of an internal data breach can be hard to surmise just by looking at the numbers alone. The following are some of the biggest internal data breaches which have occurred due to employee error:

FedEx - 2018

In February 2018, an unsecured FedEx Amazon S3 data bucket was found online. The data bucket was publicly accessible and contained around 100,000 files. These files had the personal information of everyone who used Bongo International's services from 2008 to 2015. Interestingly, Bongo International had been acquired by FedEx in 2014, but FedEx made no move to secure the information properly. It was definitely a major oversight by employees, particularly in their IT and security department.

GoDaddy – 2018

In July 2018, another unsecured Amazon S3 data bucket was found online. It contained sensitive data from GoDaddy's infrastructure in the form of spreadsheets. The most notable was a 17MB Microsoft Excel sheet with rows and rows of information. Around 31,000 of GoDaddy's systems were exposed online through that single sheet. The error has been linked to negligence in proper storage that was caused by an AS3 employee.

Australian Red Cross – 2016

In 2016, the Australian Red Cross suffered an internal data breach. A file containing personal information of around 550,000 donors was found on a third party contractor's website. The file was publicly accessible. Luckily the error was quickly corrected and all involved individuals were notified. The source of the breach was also found to be an internal employee error by the third party contractors the Australian Red Cross was working with.

Equifax – 2017

In 2017, Equifax suffered one of the biggest data breaches with over 143 million people being affected by it. In the breach, around 209,000 numbers for credit cards were exposed along with personal information of around 182,000 people in the U.S. alone. Due to Equifax's global services, their clients from U.K. and Canada also faced risks. The cause of the breach was chalked up to employee negligence from their IT and technology departments. Despite being given warnings repeatedly, they chose to ignore them instead of updating the security system.

There Are Lessons And Room For Improvement Here!

In the case studies mentioned above, all the internal data breaches occurred because of unintentional employee error. Many occurred because employees were not aware of the consequences of their actions. Organisations are being called upon to take active measures and try to reduce employee error that causes internal data breaches.

Suggested Practices To Minimise The Unintentional Insider Threat

If you are going to try and effectively reduce the risk from accidental threats, then your organisation needs to focus in shaping the behaviour of your insiders. This needs to be done using positive and negative incentives. Now, there are many factors that can contribute to the effectiveness in shaping human behaviour but in this article, I will only outline three areas:

1. **Security Policies** - The traditional approach by organisation (negative incentives) is to use policies to articulate the strategy that will define the working culture and the behaviour that is expected of the organisation employees. Now, that's all well and good, but according to CEB Research (now Gartner) conducted in 2016 revealed that more **than 90% of employee violate policies designed to prevent data breaches.**

A large number of incidents that could be attributed to an accidental insider are often the result of policies within the organisation that are either poorly defined, incomplete, not properly disseminated, nor reinforced.

Organisations need to develop a set of policies that are:

- Clearly articulated – They are precise; They are concise; They are coherent; simple to understand
- Consistently enforced – Must be adopted by all;
- Need to be relevant – Adopt the ”KISS Principle” – Keep it simple, stupid. Policies work best if they are kept simple and relevant;
- Need to be regularly evaluated and reviewed for its effectiveness; And
- Referenceable – Make it easy for employees to seek further clarification
- Regularly communicated – So that it stays in front of people’s mind.

2. **Effective Monitoring** – A proverb attributed to retired US Navy Admiral Hayman G. Rickover stated that “*You don’t get what you expect, only what you inspect*”. Having a useable and functional set of policies does not mean that it is how things are actually done or followed. There must be away of monitoring that confirms this. How else would you know whether your policies are effective or even followed?

3. **Employee Engagement** – Traditional security practices places constraints on users, their behaviour, and detect and punish misbehaviour. Such negative incentives attempt to force employees to act in the interest of the organisation and when relied on excessively, can result in negative unintended consequences.

   Positive incentives can complement traditional security practices by encouraging employees to act in the interest of the organisation. Positive incentives create a work environment where employees are internally driven to contribute to the organisation only in a positive way. Evidence suggest that not only can it deter insider misbehaviour in a constructive way, it can also reduce unintentional threats.

Get Our Help

If you are looking for a company that specialises in helping you to minimise the “human element” risks for your organisation through specialised security assessments, workshops, employee trainings and more, get in touch with CommsNet Group.

Your Next Best Step

If you are now keen in addressing the risk from within, why not attend our free public Insider Threat Worksop. These half day workshop are conducted in most capital cities and are designed to help you understand the best practices that can be implemented to identify and mitigate insider threat within your organisation.

We also provide a customised Insider Threat Workshop specifically designed for organisations. It differs from the public workshop by because it is tailored to you. The actual workshop consists of two days where we help your team develop a strategic action plan to address the risks of inside threat in your organisation.

To find out more about our Insider Threat Workshop

Contact Us

if you need some more resource material, download the Insider Threat eBook by CommsNet Group, completely free of charge. For more information, you can also send them an email at: info@commsnet.com.au OR give us a call at: +61 26282-5554.