By Boaz Fischer on May, 5 2017

ARE YOU OK WITH YOUR NEXT DATA BREACH?

Would you accept your next data breach? Of course not!

So, let me start by stating the following statement. Data security is about placing the appropriate security controls to achieve confidentiality, integrity and availability on your organisation assets in order to prevent a possible breach.

However, most organisations are confused with this philosophy. The principles of confidentiality, integrity and availability are not balanced.

What do I mean by that? Most organisations spend huge amount of investment and resources on security technologies seeking high levels of “availability”, because that’s what service levels agreements are built on.

Funny enough, organisations mistakenly focus mostly at “availability” for good security practice and that is a recipe for disaster.

Let’s take a look at the example of the Australian Bureau of Statistics (ABS) that suffered a so called Denial of Service Attack on its Census website back in August 2016. Thousands of Australian were prevented from taking part in the census (including myself) which overloaded the website.

Attacking “availability” certainly put a dent into this Government led initiative that was highly embarrassing and may have placed any future online projects on hold such as online voting for many years to come.

Importantly, the resulting consequence from the fallout of this Census fiasco has placed the Australian public lacking confidence with Government led initiatives.

October 2016: The Red Cross Data Breach

The personal data of 550,000 blood donors that includes information about their names, gender, date of birth, address" has been leaked from the Red Cross Blood Service.

This should NEVER have happened for an organisation like Red Cross Blood Service which is responsible for taking care of very sensitive and personally identifiable information, unfortunately, it did.

We all mistakes, we’re human. However, leaving sensitive data on a public exposed web server is as bad practice – It’s as bad, some may say as irresponsible as it gets when it comes to security fumbles.

Where are the necessary controls and checks?

The ramifications of the spill of donor data range from identity theft to possible blackmail. Worse still, people could be dissuaded from donating blood if they fear their details won’t be kept safe.

A breach of “confidentiality” is serious. Lives are at stake and many executives of similar organisations which hold very sensitive information just do NOT understand the ramifications.

What is alarmingly serious, most organizations do not understand where their key data is, let alone what it is and how sensitive it is. Another recipe for disaster.

Yes, digital collaboration is at the heart of every business process - files are created, stored and shared at a rapid pace. But it seems nearly impossible to keep track of who has and needs access to all of this information, and who doesn’t.

Organisations tend to think their data access is under control, but dig a little deeper and holes start to appear. Most organizations grant access readily, yet revoke it infrequently. So, don’t assume that only the human resources group can see the human resources data, or that an employee who left the company last month had all her permissions revoked. This rarely is the case.

The next case in point, **Wells Fargo Bank**, the second largest bank in the U.S., deceived over 1.5 million of

Latest Posts

Nov, 10 2020
When It Comes To Security Simplicity Is Always Better Than Complexity
Sep, 17 2020
The Risks Of Employee Layoffs And What You Can Do About It?
Jun, 1 2020
The Five Biggest Fallacies About Intellectual Property Theft

Resources

✓ **Our experts show their knowledge and insights.**

Blog | Articles | Download the Book

About the author

Boaz Fischer is the CEO and founder of CommsNet Group and a recognised leader in promoting and addressing security best practices, awareness and governance. Boaz has written over 50 security articles that are freely available online that with security trust, cloud, mobile, social media and much much more.

Americans over many years. Imagine paying fees on a ghost account you didn’t even sign up for? The phony accounts earned the bank unwarranted fees and allowed Wells Fargo to boost their sales figures and make more money in fees and commissions.

The way it worked was employees moved funds from customers' existing accounts into newly-created ones without their knowledge or consent.

The scope of the scandal is shocking. Over 5,300 Wells Fargo employees have been fired. The CEO stepped down. Wells Fargo slapped with a $185 million fines. And plenty of reputation damage to deal with.

Let’s be clear, the attack on “integrity” is very difficult to spot. Hidden within the large volume of daily system changes are the few that can impact the organisation operations and viability. These include unexpected changes to a file’s credentials, privileges, hash value, changes that cause a configuration’s values or ranges and properties to fall out of alignment with security policy.

Which brings me to my final point. In a recent survey conducted by CEB revealed,

90% of employees violate policies designed to prevent data breach.

When conveniences and productivity are chosen over security, employees put sensitive data at risk. It’s no surprise to see employees will often try and work around controls.

Verizon 2015 Data Breach Incident Report stated, 90% of all incidents are people related. Whether it’s goofing up, getting infected, behaving badly, or losing stuff.

People are the greatest risk to organisations.

Therefore, our focus in protecting our assets, must address confidentiality, integrity and availability in equal measures. More importantly, it must address the user risk.

This is not a technology problem but a people problem.

What can you do about PREVENTING INTERNAL DATA BREACHES?

If you want to place the appropriate plans to mitigate these internal threats, known as ‘ Insider Threats ’. you must approach it from a strategic point of view.

A tactical approach or a silver bullet solution as we have seen in some of the above examples, only partially works and usually adds to the overall costs without really providing return of investment or a long-term solution.

Therefore, the best approach is to develop and implement an Insider Threat Program.

The key components of an Insider Threat Program are necessary to prepare organisations for handling insider attacks in a consistent, timely, and quality manner.

If you want to address the confidentiality, integrity and availability on your assets, you must address Insider Threats in equal measures. An Insider Threat Program provides a robust, repeatable set of processes that organisation can use to prevent or detect suspicious activity and to resolve malicious incidents.

Need Help To Implement an Insider Threat Program?

If you are you looking to place appropriate Internal Security Controls to mitigate Insider Threats, and are not sure where to begin, CommsNet Group can certainly help you. This is what we do.

CommsNet Group team has many years of experience delivering improved internal security plans ranging from; Insider Threat workshops, Insider Threat Assessments, Insider Threat Hunting to helping organisations build a comprehensive Insider Threat Program.

To learn more about CommsNet Group services, please Click on the link below to contact the:

Insider Threat Team
http://commsnet.com.au/insider-threat-program-implementation