By Boaz Fischer on Mar, 5 2018

IS YOUR BUSINESS IN SERIOUS RISK BECAUSE OF A ROGUE EMPLOYEE?

Do you really know your colleagues? Do you really know who they are?

Your EMPLOYEES who you believe are loyal and trustworthy members of your workforce could potentially pose a substantial threat due to their knowledge of and access to their organisation systems and information. They can easily bypass physical and electronic security measures through their legitimate means of every day work.

Consider your technical IT administrator. They have typically all the privileges to access any asset within your business. They also have the ability to hold your business to ransom. They can disable your network. They can delete sensitive and valuable information. They can steal information. They can snoop into other user's sensitive information without your notice. They can disrupt its operations. They can destroy your business should they want.

Consider the following scenario based on a true story:

A network administrator who designed and created the network for a major US city was the only person who fully understood how the network ran, but also had all the administrative passwords for all the critical assets.

After being reprimanded for poor performance and for threatening co workers, he was resigned to a different role. However, he refused to provide the passwords to his replacement and was subsequently terminated and then arrested.

The city was unable to access those critical network assets for a full 12 days. Although during that time, fortunately, the infrastructure continued operating normally, it was also discovered that he had installed rogue access points that he could log-in remotely. In addition, he had programmed the network devices to fail if anyone attempted to reset them without the administrative passwords.

Do you have an employee that is holding your business hostage?
There are many behaviour "precursors" that an individual can act prior to performing his malicious activities. Often the signs of disgruntlement is the onset of concerning behaviours in the workplace. Some examples are

- Conflict with co-workers
- A sudden pattern of missing work / arriving late / leaving early
- A sudden decline in job performance
- Aggressive or violent behaviour
- Sexual harassment
- Poor hygiene

Some of these behaviour changes are as a result of unmet expectations. Such as:
- Did not receive a salary increase or bonus
- Did not receive a promotion
- Change in their access to information
- Job dissatisfaction
- Supervisor demands
- Change in responsibilities
- Change in co-workers relations
- Work ethic
- Personal financial changes

The Hidden problems that you don't know
A problem is hidden if it is unknown by the organisation, and therefore presenting a serious set of risks that can potentially compromise the organisation business.

1. Many of the insider offenders were clearly heading down termination through an escalation of series of concerning behaviours and associated sanctions. But when this offender left, organisations thought that the problem had disappeared with their termination. Unfortunately,

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.

the problem persisted because, they had no visibility that this offender had setup remote backdoor accounts, installed rogue software on the network, downloading malicious code/tools and installing remote network administrator tool.

2. Often organisations would try and sanction the user for their poor behaviour and performance by demotion, changing their roles, removing their responsibilities - which only exacerbated their negative behaviour and made the situation worse.
3. Excessive trust provided to employees and inconsistent enforcement of organisation policies, allowed IT administrators to subject the organisation to “ransom” behaviour.
4. Lack of insight by CEO’s to fully comprehend the problem until it is too late and thereby placed their organisation at serious risk

Most of the insiders that do commit business sabotage on their organisation leads to serious business loss.
Consider an organisation the size of 1,000 people. Imagine if this business was shut down for five (5) business working days. The loss of business revenue is calculated as follows

Average wage (assumption)	$60,000 per year
Cost to the business 3:1 ratio - 34% wage - 33% additional cost - 33% profit	$180,000 per year
For 1,000 people, this equates to	$180 million per year
Assume 220 working days per year	$818,181 per day
Should a business shut down for 5 days, this would cost the organisation:	**$4,090,090**

Could your business sustain such a loss for 5 days? Would your business survive if it was down for two weeks? Its not surprising to read that those businesses that have suffered a security breach, did not last beyond the six months.

What can you do about it?

Here are some suggested recommended steps to minimise the potential of an internal sabotage taking place.

1. Recognise the warning signs of your people behaviour.
2. Try and alleviate the situation by using an employee assistance program.
3. Review your corporate policies and ensure people are regularly updated and educated.
4. Regularly review any unauthorised user account.
5. Regularly review role-based access in your organisation.
6. Monitor for suspicious behaviour on your network.
7. And have a solid recovery process

Need Urgent Help?

Are you experiencing a potential insider threat from one of your IT administrators? Are you currently experiencing a malicious actor within your organisation?
Extracting a bad actor requires very careful thought, planning and execution.If you wish to schedule a time to discuss how we can help you, please call us on +61 2 6282 5554 or fill your details requesting support HERE