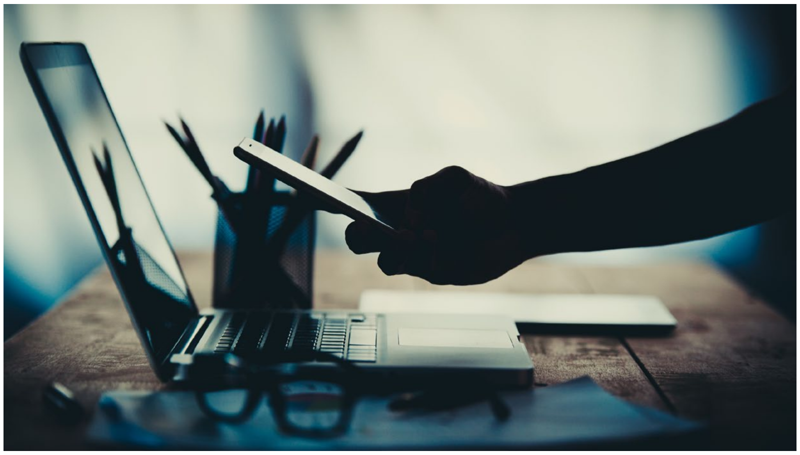
Rampart Group LLC
Investigation & Security Services

Tip *of the* Week

Insiders Threat to your Organization



Insiders – The Biggest Cybersecurity Threat to your Organization

A common misconception about cyber threats is that most attacks come from outside the organization. But that is not the case. A study by IBM found that 60% of all attacks were carried out by insiders. Companies should pay close attention to disgruntled employees upset with policies or management, workers with financial or legal problems, and employees who will soon be leaving the company.

Here are 8 tips to prevent insider threats:

1. **Review your Security Policy –** Your security policy should include procedures to investigate, document, detect and prevent misuse. It should also spell out guidelines for conducting insider investigations and outline consequences of misuse of these policies. If an employee or vendor is caught accessing privileged information, there should be consequences such as security training for minor offenses and job termination for more severe offences.

2. **Be prepared to act quickly –** If a disgruntled employee caused damage, act quickly to remove that employee's access and restore and patch weaknesses found in your systems. Also, periodically rotate and separate responsibilities among employees for sensitive operational functions.

3. **Isolate high-value systems and assets in restricted areas –** Using Key cards and PINs to restrict access to high value systems is not enough as these controls are easily defeated. PIN numbers can be given away and access cards can be lost or stolen. Biometric authentication such as fingerprint scanners are much more secure and ensure access only by the employees to whom access was granted.

4. **Use Strong Authentication –** Password cracking technology has become much more sophisticated in recent years. Longer, pre-generated passwords can be quite hard to remember resulting in employees writing them down and making it easier for others to access. Dual-authentication systems that combine a user ID and Password with a token, smart card or fingerprint reader are much more secure.

5. **Use Monitoring Tools –** Employees accessing your networks should be monitored. Network monitoring software is available that searches for predefined key words, lists and numerical formats, such as social security numbers that are leaving the network. Such software traps the data and holds it for authorization before permitting it out of network. Also consider implementing the use of surveillance cameras and keystroke logging software. Employee who know they are monitored are less likely to break security policies. Make sure you understand the laws governing your jurisdiction before implementing monitoring tools,

6. **Manage Mobile Devices –** Implement mobile device management software giving you the ability to automatically wipe data when an employee leaves the company. Be sure to notify third-party services to de-authorize former employee’s accounts immediately upon separation.

7. **Screen New Hires and check up on current employees –** The more time you spend investigating an applicant’s background the stronger and more secure your organization will be. Remember, a thorough background investigation includes screening across prominent social media platforms such as Facebook, Instagram, and Twitter.

8. **Talk to your Managers –** IT teams are focused on the technical part of the breach and not the people. Your managers are more likely to be aware of the big predictors of insider threats, such as employees who are disgruntled, under financial stress, or ready to leave the organization. Ideally, you should establish multidisciplinary teams across all areas of your organization to collaborate on identifying and preventing insider threats.

Additional Reading:
When an Employee Leaves Your Company – Protecting Your Data
10 Ways to Improve the Security of Your Computer
Protecting Your Vital Assets in a Cyber Threatened World

Call 1-800 421-0614 or visit us at www.rampartgroup.com for further ideas on protection and security. Thanks for reading!

Kathy Leodler
Chief Executive Officer
kathy.l@rampartgroup.com
(360) 981-2703

Paul Leodler
Executive Vice President
paul.l@rampartgroup.com
(360) 981-3397

Email: info@rampartgroup.com | Website: www.rampartgroup.com | Tel: (800) 421-0614