riman
RISK MANAGEMENT ASSOCIATION OF NIGERIA
Issue #83
October 2020

RISK Tips

Weekly Digest of Fundamentals of Risk Management

Helping You Understand Risk Management

Risk

"Many things in life can be safely ignored but ignoring Cybersecurity Safe Practices is an open invitation for disaster." — **JC Hunter**

Preventing Insider Threats to Cybersecurity

Ransomware continues to be a significant threat to corporate enterprises, with more attackers focusing on large companies in recent months. Threat actors are deploying sophisticated malware in well-planned campaigns that demand more expensive payments, often causing financial and reputational damage. Recently, a disturbing twist in ransomware cases has become more common: an attack either deliberately facilitated or unwittingly supported by a company employee. With an insider's help, the attack comes swiftly and with devastating impact, compelling the company to pay a large sum and spend untold hours of already scarce resources to recover.

Even as some employees are allowed back into the workplace, a large proportion may still be operating remotely. As a result, we can expect to see an increase in insider-caused information security compromises as the pandemic continues.

To better understand why this type of attack occurs and how to respond, it is worth examining what insider threats look like and what may motivate these individuals.

"Insider threat" generally refers to a security risk that originates within the targeted organization. Insiders can include current and former employees, consultants or business partners. Some may simply be negligent, used as an unwitting conduit to allow threat actors to steal company information. Other insider threats are borne of intentional acts, with someone either acting alone or with an outside threat actor. These insiders seek to hurt their employer deliberately, leveraging their position, knowledge and access to cause damage.

In the case of the intentionally malicious insider, some of the common motivating factors include money, politics and emotion (e.g., frustration, depression, boredom). As more companies lay off employees to survive COVID-19, emotions are running high. Many workers are angry. Others face acute financial constraints that could make them more susceptible to outside actors looking for a way in. Those workers who have suffered a pay cut or lost their job altogether may behave in ways they never would have otherwise considered and seek to lash out at their employer.

In addition, given the politically charged landscape around COVID-19, some employees will disagree with their employer's decisions about returning to work, and may act out accordingly.

The increase in non-intentional insiders may be driven by a lack of technological savvy, a desire for convenience or misplaced or inadequately protected devices. In the first months of the pandemic, companies took employees accustomed to working in an office with IT support staff nearby and abruptly shifted them to working from home. Companies introduced or became more reliant on technologies that many employees were not fully skilled at using, to the detriment of security. Couple that with the exponential surge in cyberattack activity observed since the beginning of the pandemic and threat actors who are always looking to take advantage of a crisis, and the odds for a successful attack likewise increase.

For convenience, employees are turning to "shadow IT" (unauthorized applications) more than ever. With entire workforces now either remote or on-site with staggered schedules, employees will inevitably resort to what is available and convenient to help get their work done, Googling for a quick fix and downloading potentially dangerous solutions.

Now that all or most of an organization's employees and other business partners are not operating from secure office spaces, misplacing or simply failing to protect devices while working remotely is also a real hazard. Consider an employee who leaves a home computer used for work open and accessible to roommates who could see confidential information, or family members whose internet activity could leave the machine vulnerable to malware.

These factors create ideal circumstances for a dramatic increase in insider threat activity. Companies can address the increased threat by taking proactive steps, such as:

- Implementing monitoring, detection and response tools to promptly identify or even stop anomalous, suspicious activity

riman
RISK MANAGEMENT ASSOCIATION OF NIGERIA
Issue #83
September 2020

RISK Tips

Weekly Digest of Fundamentals of Risk Management

Helping You Understand Risk Management

Risk

"Many things in life can be safely ignored but ignoring Cybersecurity Safe Practices is an open invitation for disaster." — **JC Hunter**

- Deploying policies and controls that disallow the use of unauthorized tools
- Monitoring employee activity, such as tracking email traffic, and using data loss prevention tools to log files accessed (after consulting with an employment lawyer)
- Increasing employee training, with a specific focus on cybersecurity challenges associated with remote work

Companies that leverage their resources to anticipate insider threats and defend against them before real damage stand the best chance of mitigating this growing risk.

Source: RIMAN, Wikipedia,RIMS

RIMAN Upcoming Programmes

ICAAP & Stress Testing	15th – 16th October, 2020
How To Use ISO 27701: Privacy Information Management System (PIMS) To Comply With Nigerian Data Protection Regulation (NDPR)	30th October, 2020
Business Continuity Management Post COVID-19 regime	11th November, 2020

Kindly contact us on Tel: 0814 241 0241 or 0802 851 6377 email: info@rimanng.org, 15 Blessing Kayode Estate, Divine Mercy Close, Off Kayode Animashaun Street (Road 15), Off Admiralty Way, Lekki Phase 1, Lagos.
Follow us: Linkedin: rimanng Twitter:@rimanng Facebook: rimanng