Top 3 Information Security Risks to Know About in 2019

Devolutions

APPLYING INFOSEC PRACTICES AND SOLUTIONS IS THEREFORE IMPORTANT TO THE SURVIVAL OF ORGANIZATIONS

Information Security (InfoSec) is the only thing that stands between your information and data catastrophes. Most attacks nowadays target data due to the increasing importance it has on the survival of organizations. You can lose your data to accidental malpractices or to malicious actors. Either way, you will face financial, reputational and existential consequences.

Applying InfoSec practices and solutions is therefore important to the survival of organizations. Organizations that use SecOps to turn security into a cultural effort gain the advantage of covering much of the security perimeter. This ensures that data remains protected at all times. Read on to learn more about InfoSec and the top three pressing data risks.

What Is Information Security (InfoSec)?

Information Security (InfoSec) is the branch of cybersecurity responsible for protecting usable data. InfoSec encompasses numerous business practices and security tools, each dedicated to protecting sensitive business and user information from unauthorized modification, disruption, destruction and inspection.

The Importance of Information

There used to be a time in which information rested squarely on an on-premises data center or physical archive. Organizations employed security guards to keep a close watch on the facilities that housed their data. Back then, data security may not have been easy, but it was certainly simpler.

In the information age, every byte of data counts. Organizations can leverage their data for making data-driven decisions based on facts rather than intuition. They can deliver the exact solution any given customer is looking for, sometimes even before the customer knows they want or need it. Organizations can turn their information into an educational hub that serves personnel and customers alike. Used wisely, information can chart a decisive path to business success.

The Consequences of Data Loss

Information is power. In the wrong hands, it can be used to wreak irreparable damage. The average cost of a data breach is $3.9 million, according to IBM's 2019 Cost of a Data Breach Report. In addition to financial losses, organizations that suffer from a data breach often face reputational damages when the data breach is exposed.

Some businesses, like Equifax, survive the fallout of a data breach. Others, like Cambridge Analytica, are forced to file for bankruptcy following a data breach event. Both companies had to pay hefty fines. Both companies also suffered severe reputational damage, as the Internet exploded with talk of the breach. One company still stands while the other closed its doors.

The Importance of InfoSec

The goal of an InfoSec operation is to protect you from any kind of data loss, including:

- **Data breach** — An attack instigated by an outside actor that "breaches" the security perimeter and gains access to your data. The actor can then steal the data, block your access to the data, corrupt the data, delete the data, or use it to launch another attack.

- **Data exfiltration (a.k.a. data theft)** — An attack that sends unauthorized actors, such as malware or bots, to copy, transfer or extract data from your network. The actor can then ransom the data or offer it to the highest bidder.
- **Data corruption** — The intentional or accidental corruption of data by internal actions or external actors. For example, the deletion of files and systems, the injection of malware or the replacement of data with misinformation.

A holistic InfoSec operation employs best practices and dedicated solutions for protecting data from the three data loss events.

Top 3 Information Security Risks to Know About in 2019

The following lists three types of attacks that threaten organizations on a daily basis, along with the type of InfoSec solutions that can help you protect against these data loss events.

1. Ransomware

A ransomware attack targets the victim's data. The threat actor injects ransomware, which is a type of malicious software that blocks the victim's access to the data. The actor then threatens to publish or forever hold the data until the victim pays the ransom demanded for the data's release.

Ransomware can occur when victims download malicious email attachments or infected software apps. It can also be injected through compromised websites or infected external storage devices. Either way, once the ransomware is there, the actor gains control of your data.

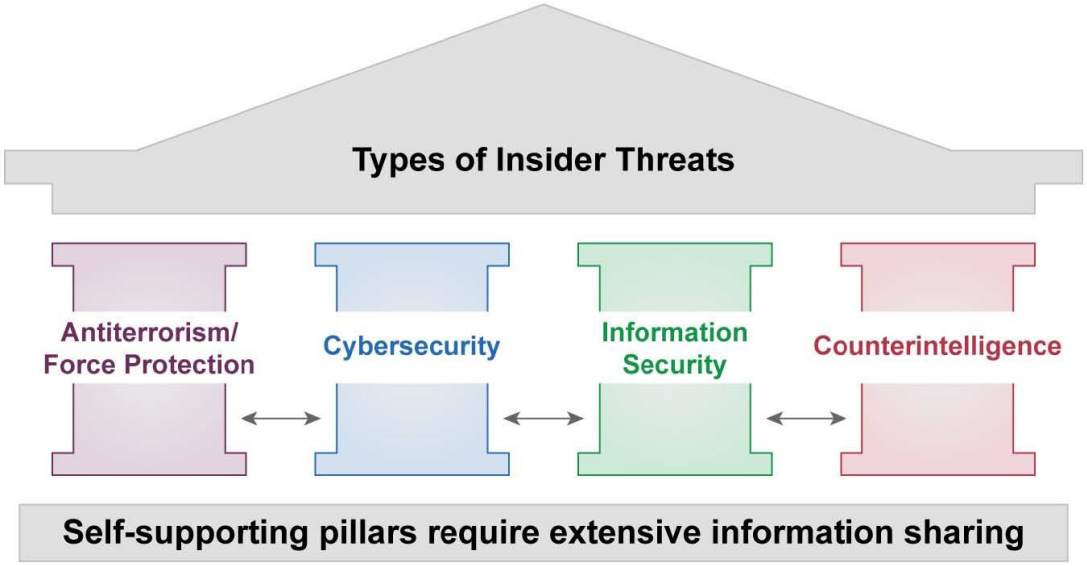
Application Security for Ransomware Prevention

The most important InfoSec action you can apply to prevent ransomware prevention is backup. If you have a version of your data safely stored away from the breached area, you won't have to start over if paying the ransom isn't an option. You could restore your operations with any of the versions you have backed up. In addition, a firewall can help prevent ransomware attacks by blocking downloads or injections from suspicious sources.

2. Insider Threats

Insider threats are individuals who threaten the data from within the organization. They make use of their credentials to cause data loss or instigate data breaches. Insider threats are generally divided into two distinct categories:

- **Accidental insider threats** — Individuals who unintentionally cause data losses. These can include deleting important files, introducing vulnerabilities to the network after clicking on malvertising, or revealing sensitive information after falling prey to phishing schemes.
- **Intentional insider threats** — Individuals who deliberately cause data losses. These are usually disgruntled employees or victims of blackmail. Sometimes they are targeted by external actors who use them to gain access to the data. Often, they are ex-employees who retain access to company files for long enough to steal business information.



Source: GAO analysis of Department of Defense (DOD) information. | GAO-15-544

Cloud Security for Preventing Insider Threats

Nowadays, most company data are in the cloud. Companies give employees and third-party entities remote access to relevant company data. Cloud security practices and tools ensure that your data is secured in the cloud.

At a minimum, this includes compliance with the General Data Protection Regulation (GDPR), which requires the anonymization of sensitive data. You can also use an Identity and Access Management (IAM) system to enforce role-based access control (RBAC) and deploy an Endpoint Detection and Response (EDR) solution to gain visibility into endpoint activity.

3. Cryptojacking

Cryptojacking, or cryptomining, is an attack that gains unauthorized access to computing resources and uses them to mine cryptocurrency. The threat actor tricks computer users into downloading malware that in turn

loads cryptomining code on the computer, utilizing malvertising, phishing, and drive-by download attacks. Once the crypto malware is loaded, the actor uses the hacked computer as a computational resource for mining cryptocurrency.

SecOps for Preventing Cryptojacking

SecOps is a methodology that unifies security with IT operations. The goal is to ensure that the software is secure through every stage of its lifecycle — from the development stage in which the codebase is written, through testing and deployment, to continual maintenance of the software.

This means that security turns into a cultural effort, which includes all of the personnel and third parties that come into contact with company data. This way, you'll have the chance to prevent and block cryptojacking attacks at all stages. Employees who are kept aware of cryptojacking dangers will be less likely to introduce crypto malware into the organization, and SecOps teams will get the chance to release security updates on a continual basis.

Conclusion

In today's data-oriented business landscape, InfoSec is vital to the survival of every organization. Anyone can fall prey to information security attacks that result in data loss. You can reduce the risk by applying a set of tools and practices to deal with threats ranging from insider threats to ransomware to cryptojacking.

To enforce security at all levels, organizations can adopt the SecOps methodology. Security then becomes an enterprise-wide effort, which involves a cultural transformation to deploy holistic InfoSec solutions and practices.