Your organization's resources are targeted

Level up the attacker's playing field and reduce the aftermath.

What Organizations are lacking in their security strategy?

Security to any firm is so crucial, we are the information gatekeepers at all times.

Institute of Forensics & ICT Security | February 2022 www.forensicsinstitute.org

Forensics & **Cyber Security** Newsletter

Your source of forensics, security and fraud insights

INTRODUCTION

Cybercrime is a constant business: Three business areas to watch out for!

"Malicious attackers take advantage of the health crisis to craft targeted emails in order to divulge sensitive information from key staff at different levels of information access. With such carefully-tailored strategies, cyber-attackers are becoming more agile and sophisticated and increase the effectiveness of their actions,"

Due to the ever-growing threat landscape in the digital ecosystem, your business must embrace cybersecurity irrespective of the size of the company. The statistics regarding data breaches on all business sizes show that the aftermaths of the data breaches are even becoming worse.

According to IBM's recent security survey, the average cost of a data breach rose from $3.86 million as was in the previous normal years to $4.24 million in 2021. This marks the highest average total cost of a data breach ever reported in history. Revenue loss impacts are significantly lower for organizations with a more mature cybersecurity posture. And higher for organizations that have not prioritized some areas such as cybersecurity. IBM's report elaborates that it takes organizations an average of 287 days to identify and contain a data breach. This is seven days longer than in the previous reports. This means that once an organization was hit on February 1, it took 287 days on average to identify and contain. The breach wouldn't be contained until November 14.

Read More>>

—CYBER SECURITY

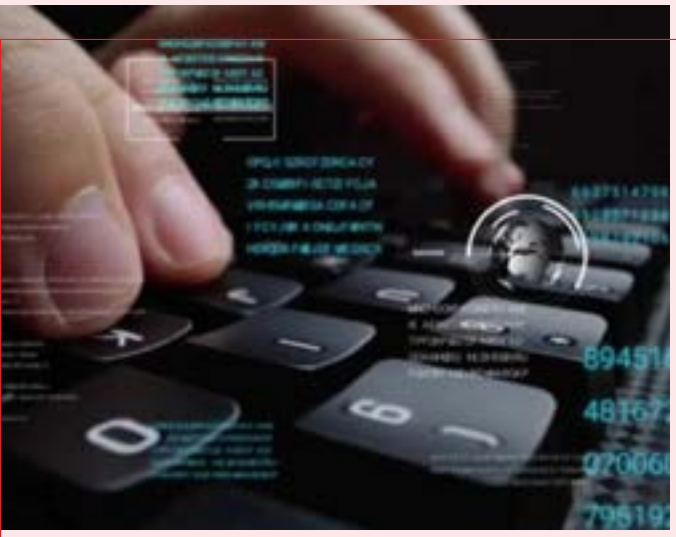
Your organization's resources are targeted: Level up the attacker's playing field and reduce the aftermath.

Organisations in the digital ecosystem spend millions trying to establish controls around their corporate networks from data breaches. This to a great extent does not phase away from the fact that breaches still occur even to the most secure infrastructures.

This to a great extent does not phase away from the fact that breaches still occur even to the most secure infrastructures. Taking a look at the incidents in the past, high profile breaches target giant firms such as Solar Winds, Marriot, Fastly, Colonial Pipeline, Electronic Arts (E.A) and so many others whose sensitive information was stolen and had major economic and security-related impact alongside reputational risks.

Malicious attackers with little failure infiltrate email servers, file servers, core systems to organizations through unknown/unpatched vulnerabilities and open doors to tones of confidential data. This is Data are the sensitive records that giant companies like Marriot, Microsoft and government entities among others collect from their customers and citizens. Such data always include email addresses, passwords, social security numbers etc.

> It's not clear why systems for organizations that have set aside security budgets and adequate controls are still compromised. Is it a question of limited resources in some organizations, could it be a question of the skills gap in cybersecurity or expertise and or inadequate budgets in some organizations?



> To this end, organizations should consider automating business security processes and integrating them in business operations. This will reduce the likelihood of intrusion towards critical resources. You also be mindful of adopting cybersecurity in your business processes. You are a target at any time.

As the digital ecosystem is scaling every time, so are adversaries who have now found it easy to use automated& AI-driven tools to profile the security landscape of the target systems and penetrate and attack corporate networks with ease.

1. Levelling the playing field for attackers. With increasing cyber incidents, organization security teams face a couple of challenges from social engineering attempts, Advanced persistent threats (APT), Ransomware attacks Unpatched systems, supply chain risks among other cyber challenges.

2. Train/Educate and prepare your entire organization. With the ever-evolving threat landscape, organizations should find it necessary to create a strong security culture starting with training staff with basic security knowledge on how to identify, predict, and protect company information security systems.

3. Empower your Incident Response Team. During an attack, the incident response team should be well equipped and knowledgeable about cybersafety and prepared to respond. The response team should be proactive and provide top management with a strategy to mitigate attacks. The team files incident reports that top management benchmarks to make ongoing decisions on enforcing a security culture.

4. Automating security practices. During an attack, the incident response team should be well equipped and knowledgeable about cybersafety and prepared to respond. The response team should be proactive and provide top management with a strategy to mitigate attacks. The team files incident reports that top management benchmarks to make ongoing decisions on enforcing a security culture.

5. Automating security practices. Much as attackers also automate their reconnaissance and target risk profiling to better understand the target and the weaknesses. Automation could also likely be a big part of the solution. Regardless of the industry or application, automating tasks allows businesses to concentrate on more productive problem-solving network defending activities. Additionally, these problem-solving activities foster innovation and can

Read More>>

—PHYSICAL SECURITY

What Organizations are lacking in their security strategy?

Why your organization would need Physical security compliance?

Security to any firm is so crucial, we are the information gatekeepers at all times. We are the protectors of the organization from all threats; regardless of whether they are malicious, internal, or environmental. We need to be vigilant and confident that the work we are doing will be regarded as a necessary operational function for the overall security and the protection of the company asset. Organizational assets may be categorized as employees, information, and intellectual property. Protection of these three things is the cornerstone of our profession.

> Protecting company data, sensitive and high priority information, corporate networks, software, company equipment, and personnel is what makes physical security. Physical Security is affected by two factors and these are; natural attacks like fire, flood, power fluctuations, etc.

What are some of the common physical security threats in your environment?

While organizations establish security strategies, it's good practice to establish a physical security plan for either their existing property or new-build. The Organization should bear in mind the common physical security threats and vulnerabilities, and how the different types of physical security threats should be encountered.

There are a variety of physical security threats in every stage of design, implementation and maintenance of the company property.

Some of the common physical security threats include; Vandalism, theft & Burglary, Sabotage and Terrorism, Unaccounted visitors, Stolen identification, Social engineering

Read More>>


ASSOCIATION OF CERTIFIED FRAUD EXAMINERS · CFE ·
CERTIFIED FRAUD EXAMINER
Join the Certified Fraud Examiner Weekend Class
0101 010 IFIS
Institute of Forensics & ICT Security
Forensics Security Training
Email: admissions@forensicsinstitute.org
Call: 0784270586/ 0708182121
www.forensicsinstitute.org
From 12th March 2022
at the Institute of Forensics & ICT Security, Ntinda
For practical skills in all the above.