TEC COMPUTER EDUCATION
www.gteceducation.com

G NEWS
The voice of G-TEC

G-TEC GCAS COLLEGE FOR ADVANCED STUDIES
www.gteccollege.com

G-TEC GENSMART ACADEMY
www.gensmartacademy.com

SEP - 2019

G-TEC GROUP OF INSTITUTIONS
Corp. Office: Peace Centre, Singapore 228149

CYBER SECURITY

What is Cyber Security?

Cyber security consists of technologies, processes and controls designed to protect systems, networks, programs, devices and data from cyber-attacks. Effective cyber security reduces the risk of cyber-attacks and protects against the unauthorised exploitation of systems, networks and technologies.

Cyber security definition

Cyber security is often confused with information security.
Cyber security focuses on protecting computer systems from unauthorised access or being otherwise damaged or made inaccessible.
Information security, is a broader category that looks to protect all information assets, whether in hard copy or in digital form.
In recent years, cyber security has fallen under media scrutiny. This can be attributed to a rapid increase of attacks, and the substantial impact to organisations.

THE THREE PILLARS OF DATA SECURITY

Robust cyber security addresses people, processes and technology.

People

There are two key aspects to the people element of the trinity that you need to consider. First, everyone in the business needs to be aware of their role in preventing and reducing cyber threats, whether it's handling sensitive data, understanding how to spot phishing emails or the use of BYOD. Cyber security is a business issue and everyone has a role to play. An effective security awareness programme can help reduce the risk of cyber threats aimed at exploiting people.

Secondly, there are the specialised technical cyber security staff. They need to be fully up to date with the latest skills and qualifications to ensure that appropriate controls, technologies and practices are implemented to fight the latest cyber threats. Cyber security staff who don't stay up to date affect the organisation's ability to mitigate and respond to cyber attacks.

Processes

Processes are key to the implementation of an effective cyber security strategy. Processes are crucial in defining how the organisation's activities, roles and documentation are used to mitigate the risks to the organisation's information. Processes also need to be continually reviewed: cyber threats change quickly and processes need to adapt with them. But processes are nothing if people don't follow them correctly.

Technology

Technology is obviously crucial when it comes to cyber security. By identifying the cyber risks that your organisation faces you can then start to look at what controls to put in place, and what technologies you'll need to do this. Technology can be deployed to prevent or reduce the impact of cyber risks, depending on your risk assessment and what you deem an acceptable level of risk.

Why Is It Important to Address Cybersecurity Threats?

Most enterprises have come to understand the importance of addressing internet security. With nearly two-thirds of a recently surveyed group of small organizations having experienced cyber-attacks in the last two years, the risks of a lack of cybersecurity are becoming more widely talked about. These risks include:

- **Compromising of private data**. Companies today rely heavily on the data they collect, whether it's market information, various account details or the personal information of customers. If a cyber-hack occurs, not only is there a chance for this information to be stolen by another entity, but data could also be altered in a way that drastically damages the company's operational reliability.
- **Costly recovery expenses**. Not only does a breach in security put information at risk, but there are also potentially devastating financial repercussions. Most of these are in the form of "hidden" costs that can continue to impact your business for up to two years after the incident. Whether it's in the form of new IT training, acquiring new software or the lengthy process of restoring lost data, the loss of both time and money can be devastating.
- **Weakened client trust**. Naturally, customers don't like hearing that their personal information has been compromised. After a cyber-attack occurs to a company that they originally trusted to keep their data safe, consumers may decide to discontinue their business and seek services elsewhere, tarnishing not only the reputation of the attacked company but also reducing its bottom line.

To prevent these losses, we need to pay special attention to what leads to these online security incidents. Nearly 90 percent of data breaches are caused by a human-made mistake or behaviour, and further data from the survey mentioned above suggests that employee ignorance is one of the leading contributors, manifesting itself in a few different forms:

- **Widespread lack of understanding and training**. It's not only the IT department who can accidentally expose the company to online intruders. but also many tech support employees are not necessarily cybersecurity experts, which should be addressed more extensively, other non-technical employees also carry the responsibility to behave wisely online. If the workforce has a generally limited knowledge of what threats look like, leading employees to find themselves opening emails tagged with malware or accessing unsecured networks, even prepared IT departments can't defend the company properly.
- **Lack of their groundwork for new IT initiatives**. In 27 percent of survey respondents, new IT policies contribute to the lack of preparation for security incidents. Say the organization implements new cloud computing initiatives or adopts new user controls without adequately building foundations and training employees effectively. Then this can lead to an absence of awareness, user errors and even the initial installation of software without ensuring the right security settings are in place, opening the company up to impending threats from the start.
- **Overwhelmed technical departments**. Another critical factor in addressing cybersecurity is acknowledging that overworked IT departments are less adequately prepared to tackle cyber-attacks head-on. Understaffed or underskilled groups within small companies might be those best suited to look into outsourcing business network security solutions to help maintain proper defences.

We can begin to take steps toward better cybersecurity solutions by providing a greater understanding of online threats, what they entail when they occur and how to detect them. Let's start by looking at the different types of cybersecurity threats that businesses can face today.

What Are the Most Common Cybersecurity Threats?

Today, cyber-attacks can come from a variety of places and in a variety of forms. Some types of threats are more invasive than others, but they can all be equally jarring if left unprepared. A few of the typical attackers and sources of cybersecurity threats include:

- Organized crime groups
- Competitors of your business
- Hackers
- Terrorists
- Foreign governments

While these sources are all coming at the company from the outside, another considerable threat that we face is inside attacks, often perpetrated by a disgruntled employee or contract worker who has been trusted with network access.

Some of these attacks are not intentionally malicious, like if a user is simply testing their limits or digging through the network to find information they don't have access to. But it's important to note that, more and more, criminal groups are incentivizing insiders to deliberately cause harm from within.

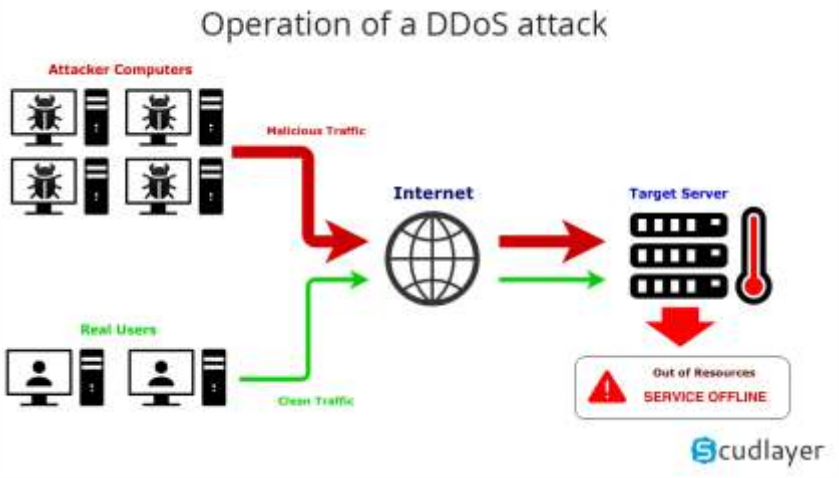
The Types of Cybersecurity Threats That We Face

The way this harm looks can vary, so we should take a moment to address the most common types of cybersecurity threats that we need to watch for, whether they are attacks coming from the outside or from within the organization itself:

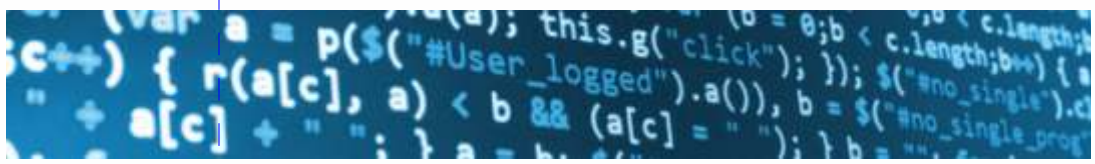
- **Phishing**. Cybercriminals will try to gain access to your secured network through different means, the most common of which is through phishing. By using social sites or email, these scammers will convince users to click on misleading links, provide sensitive information or company data, or even download content to their computer or server.

- **Malware**. If a victim of phishing does end up initiating a download, there's a good chance that the program received is harmful or malicious. A Trojan virus, for example, is a form of malware brought onto the network disguised as legitimate software, often carrying out its true purpose without the user knowing. Malware comes in various forms, tasked with anything from spying on the system to manipulating its code.

- **Distributed Denial of Service (DDoS)**. This is a type of attack that floods the server with requests from multiple sources, leading it to become overwhelmed to the point of slowing down substantially or even crashing. Once this occurs, the system becomes impossible to use effectively until theses numerous interactions are cancelled and blocked.
- **Brute Force or Password Attacks**. These threats involve an attacker attempting to gain access to a network by using a program to ascertain a working password. They're the primary reason why it's important not to use the same password across the board and why these login details need to be changed regularly.



- Internet of Things (IoT) or Algorithm Manipulation. As organizations grow to rely more and more on their wearable tech, cloud-computing industrial devices and other IoT applications, the more vulnerable their data becomes. Similarly, as automation has led companies to trust their algorithms to interpret and apply their data, they may be susceptible to threats in the form of these systems and codes being compromised without frequent monitoring and occasional human interaction.



- **Ransomware**. This is a type of malware that, when opened, locks the system down and encrypts the device so that no one can use it anymore. Ransomware is one of the most sophisticated and damaging threats out there. The computer or server affected will remain locked until a hefty ransom is paid on its behalf, although some hackers are prone to not following through on the unlocking that they promise, causing the business to suffer even further.

These are some of the most widely understood attack patterns, which only the right security software can help you detect and prevent. In addition to this list, we especially need to be aware of what is called Advanced Persistent Threats, or APTs.

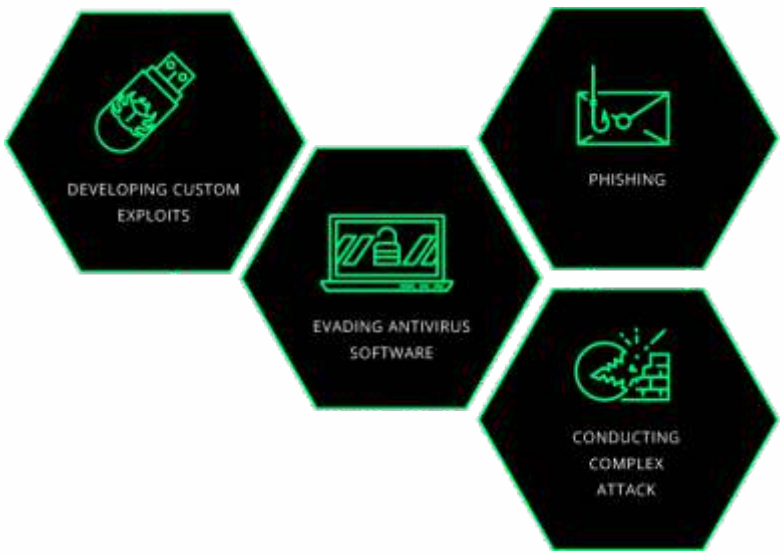
The Five Phases of an Advanced Persistent Threat or Intrusion

These threats are precisely what the name implies: extensive and aggressive, and drawn out over a long period. They are usually composed of several phases, involving a string of cybersecurity threats like the ones already mentioned. Here is what these phases can look like and what you can expect from each one:

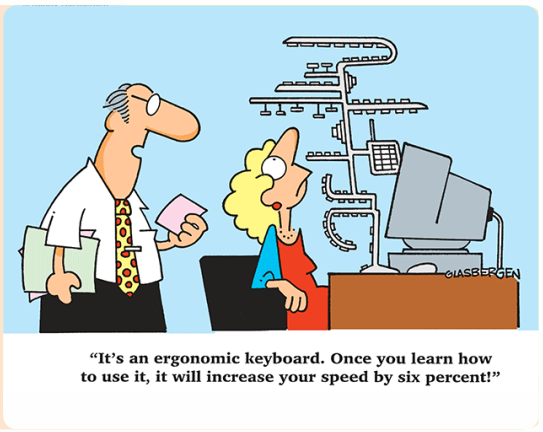
1. **Reconnaissance and Probing**. Employees who are too lazy to check for warning signs may find themselves surrendering confidential information. This phase usually involves a form of phishing that relies on this human complacency. Sometimes the hackers sit back and wait for the unsuspecting victim to visit a fake website and input sensitive info. Other instances involve a physical device being planted by an insider into one of the network's computers that will gather the data for them.

2. **Intrusion and System Compromise**. Without doing anything too suspicious, the perpetrator will then use the login credentials or other access tools to enter the flow of network traffic, seeking information to exploit or critical systems to disrupt. As they blend into the typical workings of the network, the attacker can observe activity for months from a remote location without being detected.

3. **Exploitation and Malware Installation**. The hacker moves laterally on the network, gathering additional user account data to expand their foothold and compromising sensitive files. As they go, they begin to insert forms of malware like Trojans to exert further control. They still may be weeks from detection, so the scope of the damage they cause during this phase can take years to discover and repair after the attacker is expelled.



Smile Corner



"It's an ergonomic keyboard. Once you learn how to use it, it will increase your speed by six percent!"

4. **Data Capture or Manipulation**. Next, the hacker will begin to decrypt and remove information from the system that has been infiltrated. Decryption is a process that takes time and skill, but if the imposter has made it this far into the attack, they are likely going to follow through with their objective.

5. **Track-Covering and Exit**. Once the attacker has what they came for, they will either leave the network, create backdoor entries so they can return undetected or even destroy the evidence using ransomware. Even after their mission is complete, unless they set off alarms or shut the system down with malware, their invasion can remain undetected while a large percentage of company data has been compromised. That's why constant visualization and remaining alert is crucial for network owners.

Preventing these kinds of persistent attacks is all about careful and continuous monitoring of your system. It can be a challenge to detect a data breach of this scale because of the attacker using valid login credentials and remaining on the down-low for months at a time. But the right tools can make a big difference in alerting you to any unusual activity.

How Can You Detect Cybersecurity Threats Before They Occur?

Typically, businesses have a few different in-house approaches to data management and protection that they resort to, from drilling their employees on compliance to installing firewalls and keeping their software up-to-date. Additional data breach detection methods vary in complexity and effectiveness:

- **Basic methods**. As a first line of defence, we can commonly incorporate a shallow stack of technologies that allow real-time correlation and logging, enabling the owner to highlight suspicious network events.

- **Emerging methods**. To go a step further, owners may incorporate history analytical capabilities, taking any action of interest and comparing current operations to previous instances when these activities last occurred. This insight allows us to establish new precedents or policies to minimize these incidents.

- **Advanced methods**. Introducing intuitive security programs prevents even insiders from conducting malicious activity without detectable deviations from standard network behaviour. It's this kind of oversight that is crucial in protecting sensitive data and avoiding the substantial losses that cybersecurity threats can incur.

The way businesses traditionally try to detect cybersecurity threats can be relatively inefficient without the right tools. Sometimes it's even dangerous, as SMBs fail to adapt to the new methods of cyber attacking that are consistently developing.

Publisher
Mehroof I. Manalody
Chief Editor
S. Thulaseedharan Pillai
AGM - Operations
Editor
Joseph M Thomas
HOD - Academics
Editorial Board
K.B. Nandakumar (General Manager)
Deepak Padiyath (Vice President & CEO GENSMART)
Ashley George Vaz (Manager Operations)
Sajindas T (Operations Manager)
Raghunath K.P (DGM-Expansions)
Anwar Sathic (Marketing Manager)
Shibida Ahamed (Technical Manager)
Raihana K (Academic Coordinator)
Email: gnews@gteceducation.com *For internal circulation only*

OUR PRIDE