# How prepared are CISOs for cyber security breaches?

**Author:**

JOSE VARGHESE,

EVP & HEAD – CYBERACTIVE℠ SERVICES

PALADION

HIGH SPEED CYBER DEFENSE

It's no longer enough to prevent cyber security breaches. Today, because of the damage & cost that follow high profile breaches, reaction time is of more importance. Because these breaches are happening on a daily basis, CIOs are obligated to take notice and ensure that they are ready for such an occurrence. What has now become essential to an adequate level of preparedness are the right tools to effect a decent reaction.

> "Where most cyber security strategies follow a rule of 'prevention is better than cure', today the most effective strategy is rather to 'cure before the point of irreparable damage.'"

Security perimeters that are constantly in place can only provide limited protection. Persistent hackers take days—sometimes weeks—to plan and execute an attack. When these attacks become apparent, it's how CIOs and cyber security teams reacted to the threat that will make all the difference. This does not mean that basic cyber security should be ignored or done away with; but rather that extra measures must be taken for times when that security is breached.

## The Importance of Continually Tracking your Company Assets

Recognising the vulnerabilities of company assets will put CIOs in the perfect position to protect them successfully. In order to do this, cyber security teams must at all times know where they stand in terms of two major realities. First of all, does the company have a relevant, up-to-date inventory of these assets? Second, is there a way to track these assets for the sake of detecting threats if and when they happen?

When these questions are asked and answered, CIOs can position themselves to respond to threats more effectively. The reason for this is because they now know what assets may be threatened, where they are located, exactly how vulnerable they are, and who has access to them. Cyber security teams are now setup to detect threats faster, and respond to them before they get out of hand.

# Fast Detection of Threats is Vital in Effectual Protection

Good security goes further than simply aiming to prevent an attack. Today, it should be expected that a breach will happen. If that breach can be detected quickly, you can be sure that CIOs will be able to do more in terms of remedying the situation. Ultimately, it's this fast reaction time that saves companies millions in revenue.

To reiterate, however, it's critical that a team of cyber security professionals have the right tools in order to achieve this early detection. One such tool is a system that scans for vulnerabilities continuously. Another is a monitoring system that diligently searches for attacks that are common to the asset in question. However, what makes all the difference is a system that also looks out for new, more developed threats.

"Because threats evolve over time, your security system should be equipped to do the same."

# Segregating Serious Attacks from the Distractions

Even with a detection process in place, many an alarm will go off at trivial incidents. That's why it's of utmost importance to separate these from the threats that actually stand to do damage. This is what's known in cyber security circles as triage. Having an effective triage will help a company's security team react to threats without being distracted by nonessential incidents. An example of where this kind of triage was needed is the 2013 attack on US retailer, Target. Over 70 million credit cards were lost. Even with the best preventative security in place, the real threat wasn't addressed until much later because so many distractions existed which threw off the security team.

"An effectual triage system is the only remedy against security distractions. It will assist CIOs and their teams to first respond to priority threats that warrant a response."

The pertinent question begs whether your triage can measure how critical a threat actually is. This requires the ability to analyse past attacker behaviour and subsequently put together a profile that can adequately respond to threats. What the security team is left with are a number of noticeable priorities that must be dealt with first. It takes an excellent real time security system to analyse all assets and their respective threats in order to come up with what needs to be dealt with first.

## Rapid Investigation is Necessary for Identifying the Remedy

Once the definite threats have been detected, your security team can remedy the situation. However, it's pointless to think that one remedy fits all. A thorough and rapid investigation must first take place to ascertain what kind of a response is called for. How an attack was carried out, when it happened, and who committed it are all questions that need quick answers in this kind of situation.

The only way to get these answers is through a system that actively collects data from multiple assets. From here, your security team should be able to recognise where the threat is coming from and how it originated. More than this, investigators will be able to identify the methodology of the attackers as well as the most practical way they can be stopped.

"Knowing when & how an attack was carried out is a sure way to identify how it can be stopped in its tracks without further loss being incurred."

# Containing the Threat in Real Time

Fast eradication of threats must be carried out if minimal damage is to be attained. Once again the right tools are essential for containment to take place effectively.

"The right tools can mean the difference between reacting to a threat in minutes versus days."

The best reactive cyber security systems can isolate a server or endpoint within minutes of a breach. It's also important, however, that a single process can be halted without interrupting the entire company system. All this must of course be done automatically and in real time. If it isn't, the threat may result in unspeakable damage for the company, its employees, and worst of all its customers.

Attacks such as these are the result of long, planned-out strategies by persistent hackers who are determined to succeed in their attack. Bear in mind that in the midst of this planning, they have thought out methods of bypassing your security and rendering your reaction pointless & ineffectual.

# Learning and adapting through past threats

Much attacker success is derived from shared information between themselves. This information may include—but is by no means limited to—cracked passwords, successful breach methods, and even tools to carry out the job. An organisation that does the same will put itself in a good position. Every time a breach takes place, a lesson makes itself available. This is the kind of adaptability that needs to be employed by high profile companies.

Companies that collect threat intelligence, such as attacker profiles and methods, arm themselves with better defences the next time around.

Through sharing mechanisms and forums, this kind of intelligence can be collected and published for the benefit of individual organisations. A smart organisation will ask itself whether this type of information is being collected & catalogued, shared on forums such as FS-ISAC or IT-ISAC, and exchanged for other useful information that can prevent a future breach.

# Conclusion

To summarise, let's explore everything that needs to be in place for effectual cyber security responses. To begin with, asset awareness must be visible & accessible to the team at all times. If any assets are added, these must be immediately identified without the chance of a gap-related vulnerability taking place. In addition to knowing where assets are, it's imperative that those same assets' weak points are understood. Knowing where vulnerabilities lie as well as what kinds of threats (new or old) may target them is a major part in protecting those assets.

Knowing about these threats is not enough. Proactive security will always search for threats on a continual basis so as to contain them quicker should they appear. During this process, real threats must be distinguished from nonessential incidents so that no time is wasted in containing serious threats when they occur. Occurrences that are serious must be investigated quickly so that little-to-no damage transpires before containment takes place.

*As quick as investigation must be, it's equally important that this investigation gives the security team enough information to react appropriately to the threat. Once the root cause has been identified, containment can take place rapidly, and any affected areas can be isolated from infecting the others. These are the steps that ultimately save the reputation of companies the implement them.*

PALADION
HIGH SPEED CYBER DEFENSE

## ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its semi-autonomous cyber platform and managed services with leading security technologies. Paladion is consistently rated and recognized by independent analyst firms and awarded by CRN, Asian Banker, Red Herring, amongst others.

For 17 years, Paladion has been actively managing cyber risk for over 700 customers from its six cyber operations centers placed across the globe. It houses 900+ cyber security professionals including security researchers, threat hunters, ethical hackers, incident responders, solution architects, consultants and more. Paladion is also actively involved in several information security research forums such as OWASP, and has authored several books on security monitoring, application security, and more.

---

**WW Headquarters:** 11480 Commerce Park Drive, Suite 210, Reston, VA 20191 USA. Ph: +1-844-507-7668

Bangalore: +91-80-42543444, Mumbai: +91-2233655151, Delhi: +91-9910301180, London: +44(0)2071487475, Dubai: +971-4-2595526, Sharjah: +971-50-8344863, Doha: +97433559018, Riyadh: +966(0)114725163, Muscat: +968 99383575, Kuala Lumpur: +60-3-7660-4988, Bangkok: +66 23093650-51, Jalan Kedoya Raya: +62-8111664399.

sales@paladion.net | www.paladion.net