CYBER SECURITY SERIES:

ACTIVE, PROACTIVE OR REACTIVE?
ASSESSING YOUR CYBER SECURITY POSTURE

CAPCO

NEED TO STAND UP TO CYBER SECURITY BREACHES MORE EFFECTIVELY? CHANGE YOUR POSTURE!

An organisation's 'security posture' indicates how robustly it is equipped to avoid, detect and repel cyber threats, based on current information security infrastructure and practices. Given ever-bolder cybercrime, a major review of security posture is now imperative.

A PROACTIVE DEFENCE STRATEGY DRIVES CHANCES OF SUCCESS AGAINST CYBER CRIMINALS

Cyber security failure costs continue increasing. High profile examples include massive breaches at Yahoo (twice), Target and Equifax. Hackers break through complex and costly defences to access and steal valuable data. They cost their victims dearly - financially and by damaging consumer trust, market profile, and even core brand value.

The three principal strategies for combatting cybercrime today are the reactive (after it happens, if it happens), the active (as it happens) and the proactive (before it happens).

The Target breach alone, where credit card details were stolen from point-of-sale machines at nearly 2,000 stores, is estimated to have cost nearly $300 million. An active cyber security strategy would have offered many routes to limiting, and potentially preventing, the damage.

REACTIVE – 'IF THEY COME, WE WILL RESPOND'

Traditionally, security approaches have centred on the detection of and reaction to threats that actually penetrate a system or network. These approaches focus on establishing strong perimeters to prevent breaches. Information security is typically a discrete operation, independent of the core business. Significantly, it is organisation-specific. It does not consider issues arising from security practice variations between different, but connected, companies.

The reactive approach invests in upgrading to latest versions of security software and 'keeping the lights on'. The downside is its limited view of the threat landscape. This is inappropriate for dealing with a '360 degree' threat horizon and is proving insufficient for effective network safeguarding. However, this type of strategy still has a place in today's cyber security environment and for some good reasons:

- **Longevity** – reactive has been around for a while and contains proven elements
- **Security software choices** – there are many reactive strategy-driven resources and options available to businesses, allowing them to choose what best suits them
- **Simplicity** – the reactive approach is relatively simpler, with limited upkeep costs.

These advantages make a viable option for businesses that do not store sensitive data. But, for organisations responsible for valuable data, events show that reactive, strategy-led defences are inadequate.

ACTIVE – 'WHEN THEY COME, WE WILL RESPOND'

An active approach to security builds upon the reactive with enhanced security monitoring of information and assets. In addition, vulnerability management, advanced firewalls, multi-factor authentication, NAC (network access controls), DLP (data loss prevention) and other technologies are deployed and managed. Security Information Event Management (SIEM) systems are also deployed to provide real-time monitoring, though often not for all enterprise-critical assets.

However, regardless of the investment in people, processes and technology, the active model still waits for the bad guy to act first, before responding. By that point, it is potentially too late, the attacker is already in, although it will be discovered sooner which means moving to active measures faster.

Another drawback with the active stance is that many companies try to protect all the data all the time, thus increasing cost and unnecessary complexity, as not all data is worth the same.

PROACTIVE – 'BEFORE THEY COME, WE WILL BE READY'

A proactive defence posture is intelligence-led, based on comprehensive cyber security assessments. It uses cyber threat intelligence feeds in conjunction with real-time network monitoring to develop a detailed picture of the whole security landscape, and how threats can be manifested and exploited. Taking into account the nature and needs of the core business at threat, the resulting in-depth analysis can help identify and remediate weak spots, before exploits are available, as well as identify areas for targeted investment to improve the total security of the system. Active intrusion prevention, data protection, data loss prevention and encryption or dynamic distribution technologies can protect data at rest, in-motion and in-use.

In this model, information and assets are assessed for confidentiality, integrity and availability needs. Defences are tuned to provide the level of protection appropriate to the value of the information and the risk appetite of the company.

The basis is strategic military principles of taking the fight to the enemy. Honeypots and (digital) tar traps can be set up to attract, slow down, or funnel attackers to certain parts of a defended but valueless network. This can help identify and act against zero-day exploits, by hindering the attacker, and then assist in identifying the attack vector so it can be addressed.

Proactive intelligence will strengthen defences and increase resilience against the effects of Advanced Persistent Threats (APT) and ensure the smallest possible attack surface for zero-day attacks. The latter allows faster detection of attacks and identification of remediation activities. Enhanced and detailed information can then be extracted and passed to the relevant authorities.

Clearly, staying one step ahead in potential attack vectors can make the defining difference. Thus, research and development are at the heart of this dynamic approach. But proactive cyber security posture does not render current firewall and safeguard infrastructure pointless.

The proactive posture is most productively implemented in conjunction with the 'traditional' defences. It builds on the active to turn the enterprise from a perimeter and defence in-depth approach to one that combines data centricity with intelligence. This in turn allows firms to predict adverse security events before they occur and take proactive defence measures.

To work effectively, this strategy demands long-term commitment. This is a challenge, given limited resources and shortage of appropriately skilled workers. (Although, over time, these obstacles will likely reduce.) But for big institutions safeguarding substantial, valuable and continuously growing data sets, the prospect of proactive - and much more effective – cyber security is increasingly attractive.

THE KEY REACTIVE, ACTIVE AND PROACTIVE SECURITY POSTURE CHARACTERISTICS – AT A GLANCE

REACTIVE	ACTIVE	PROACTIVE
Limited view of the threat landscape	Real-time monitoring and defence in-depth increases security	Cyber intelligence feeds and real-time monitoring give full overview of the threat landscape
Deals with threats once they enter the network	Detects known threats and expolits	Uses threat intelligence to proactively identify high risk and weak areas. Provides intelligence on yet to be published exploits and attack vectors
Plentiful resources and options already exist	Limited resources and skilled workers availability	Difficult to achieve, required highly-skilled staff are scarce
Investment used only to update and 'keep the lights on'	Investment decisions driven by current needs and the perceived level of security	Investment decisions driven by current needs, with investment in R&D necessary
Does not actively engage attackers	Engages attackers, as they attack	Diverts attackers through use of honeypots, tar traps, etc. Uses intelligence to identify attack vectors before they are common knowledge and increases protection against APT and zero-day attacks

WHAT CAN A PROACTIVE CYBER SECURITY POSTURE ACHIEVE IN PRACTICE?

If it had been implemented at Target, for example, many routes would have existed to prevent the damage and to provide faster means to contain and limit the damage.

Constant real-time network monitoring combined with intelligence would have identified abnormal activity from infected point-of-sale machines. This would have allowed for isolation and infection removal, before nearly 2000 machines were compromised and data was egressed.

Honeypots and tar traps would have slowed down incursions, funnelling the hackers away from the real data, and preventing large losses of confidential information.

‘Caught’ infected machines could even have been used to track down the attackers, limit their potential to carry out future attacks, and provide prosecution evidence in a legally acceptable form.

Finally, non-attributable information on systemic vulnerabilities exposed, and exploitation mechanisms used, should be shared with the cyber security community and intelligence vendors. This could help improve identification of similar attacks and strengthen resistance.

CONCLUSION

This ‘alternative Target scenario’ remains hypothetical. Yet it shows compellingly how a proactive approach is vital in effectively combatting cyber security threats.

As the cyber security industry continues to fight the war against criminals, the big hope is that there will be fewer of those massive breaches that shock the world. Making hope a reality demands a big shift – to nothing less than a fully proactive security posture.

REFERENCES:

https://www.thesslstore.com/blog/2013-target-data-breach-settled/

AUTHORS:

Kristian McCaul, Associate Consultant

Danushka Jayasinghe, Consultant

Evdokia Kardoulaki, Associate Consultant

Kian Adam Rahnejat, Consultant

Jibran Ahmed, Managing Principal

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward. Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and investment management, and finance, risk & compliance. We also have an energy consulting practice. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at www.capco.com, or follow us on **Twitter, Facebook, YouTube,LinkedIn** and **Xing.**

WORLDWIDE OFFICES

Bangalore
Bangkok
Bratislava
Brussels
Charlotte
Chicago
Dallas
Dusseldorf
Edinburgh
Frankfurt
Geneva
Hong Kong
Houston
Kuala Lumpur
London
New York
Orlando
Paris
Pune
São Paulo
Singapore
Stockholm
Toronto
Vienna
Warsaw
Washington, DC
Zurich

CAPCO.COM

CAPCO