KPMG

Targeted attack review

Be in a defensible position.
Be cyber resilient.

Cyber criminals are getting more sophisticated, targeting and gaining access to an organization’s crown jewels. Organizations need to be constantly testing and improving their security infrastructure.

Species such as the armadillo lizard have adapted to ward off threats in the most challenging environments. Organizations also need to protect, detect and respond to ever-changing threats.

How effective is your process and technology?

Increasingly sophisticated methods of cyber crime are being devised and used to gain access to critical business information and processes. This can put an organization at risk through weaknesses in their approaches for dealing with people, process and technology related risks.

What is a targeted attack?

A targeted attack aims to gain access to a specific system which typically contains an organization’s most sensitive data, or to perform an activity of some type, such as an unauthorized transaction, typically of a sizable amount. These are frequently highly sophisticated attacks that have been planned over long periods of time, often bringing together social engineering, malware and system and process vulnerabilities to gain insight into weaknesses related to the people, process and technology in an organization that they can then use to exploit their attack. These attacks can be global, national, against a defined industry or targeted to a specific organization.

Targeted attack review

A targeted attack review is a customized review created specifically for your organization. Depending on your needs and requirements, the scenarios, attack formulation and testing methods will be created appropriately.

Our approach combines techniques from intelligence and offensive security communities: the approach used by many cyber criminals.

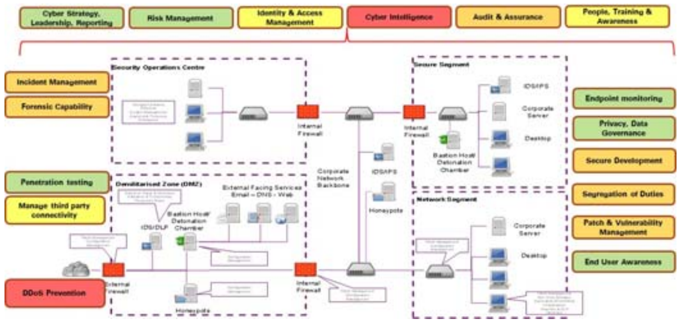
The Targeted Attack Review can help your organization determine how deep within your infrastructure a cyber criminal can penetrate and gain access to your most sensitive data, or most sensitive functions. This can involve the assessment of minor or seemingly trivial weaknesses that can be aggregated and exploited to create a material breach.

Targeted attack review provides:

- **Sensitive data/process identification:** Identify the data that is most at risk, the processes most likely to be exploited, and the weaknesses within these processes.
- **Technical review:** Understand how those seemingly innocuous technical weaknesses can be used to breach defenses.
- **People assessment:** Understand whether certain people could be a single point of failure, could be manipulated, could turn rogue after some time, and how this can be detected and avoided.

The core value is the aggregated nature of these risks to provide attack scenarios. This allows for remediation steps to be identified.

As shown in the diagram below, many organizations have complex processes and network environments with multiple entry points that are connected. Weaknesses in any parts of the process or network can allow for an attacker to exploit them and cause harm.



Customizing scenarios and attack formulation

KPMG understands the importance of an organization's crown jewels, and will customize the scenarios, attack formulations and tests. Our approach will be focused on the processes and layers of security technology around your crown jewels.

The range of tests KPMG can deploy a range from the traditional to the more sophisticated used in cyber forensics. As a result, the range of scenarios and attack formulations we can create are extensive.

Some of the tests include client side exploits, Rouge AP, web application exploits, exploits through USB, lock picking, RFID cloning, RFID Bruteforcing, 802.1x by-pass, traffic sniffing, authentication bypass, and authorization bypass.

Why choose KPMG's cyber team

We use the same tools and techniques that professional hackers use for ethical hacking and offensive security to test the layers of security for a large number of clients.

- We have carried out similar hands-on testing across various industries.
- We are industry professionals with a history of working with law enforcement and are often called as witnesses at courtroom trials.
- Our team consists of consultants and advisors to federal agencies such as the Royal Canadian Mounted Police (RCMP), the Canadian Armed Forces, the US Secret Service, the Department of Homeland Security.
- Our accredited forensic practices and over 2,700 practitioners across the world are available to support investigations spanning multiple geographies including those mandating private investigators licensees to perform forensic investigations.

Cyber Emergency?

Please contact our 24/7 Cyber response hotline

1-844-KPMG-911

1 (844) 576-4911

We believe cyber security should be about what you CAN DO – not what you can't.

Award winning

KPMG International has been named a Leader in the Forrester Research Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2016 .

The KPMG cyber team won the Information Security Consultancy award in 2011 and 2012. The team also won the MCA award in 2011 and 2012.

Independent

Our recommendations and technical strategies are based solely on what is fit and appropriate for your business.

KPMG in Canada is not tied to any technology or software vendor.

Collaborative

We facilitate and work with collaborative forums to bring together the best minds in the industry to collectively solve shared challenges and emerging threats.

KPMG's I-4 forum brings together over 50 of the world's leading organizations.

Trusted

KPMG member firms have a long list of certifications and permits to work on engagements for the world's leading organizations.

Global, local

KPMG is a global network of member firms with over 174,000 professionals in 155 countries with over 2,700 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide. KPMG's regional practices can service your local needs from information security strategy and change programs, to low level technical assessments, forensic investigations, incident response, training and ISO27001 certification.

KPMG's Cyber Team works with organizations to help prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

Contact us

Paul Hanley
Partner, National Cyber
Security Leader
T: 416 777 8501
E: pwhanley@kpmg.ca

Kevvie Fowler
Partner, National Cyber
Response Leader
T: 416 777 3742
E: kevviefowler@kpmg.ca

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. 9137

kpmg.ca/cyber