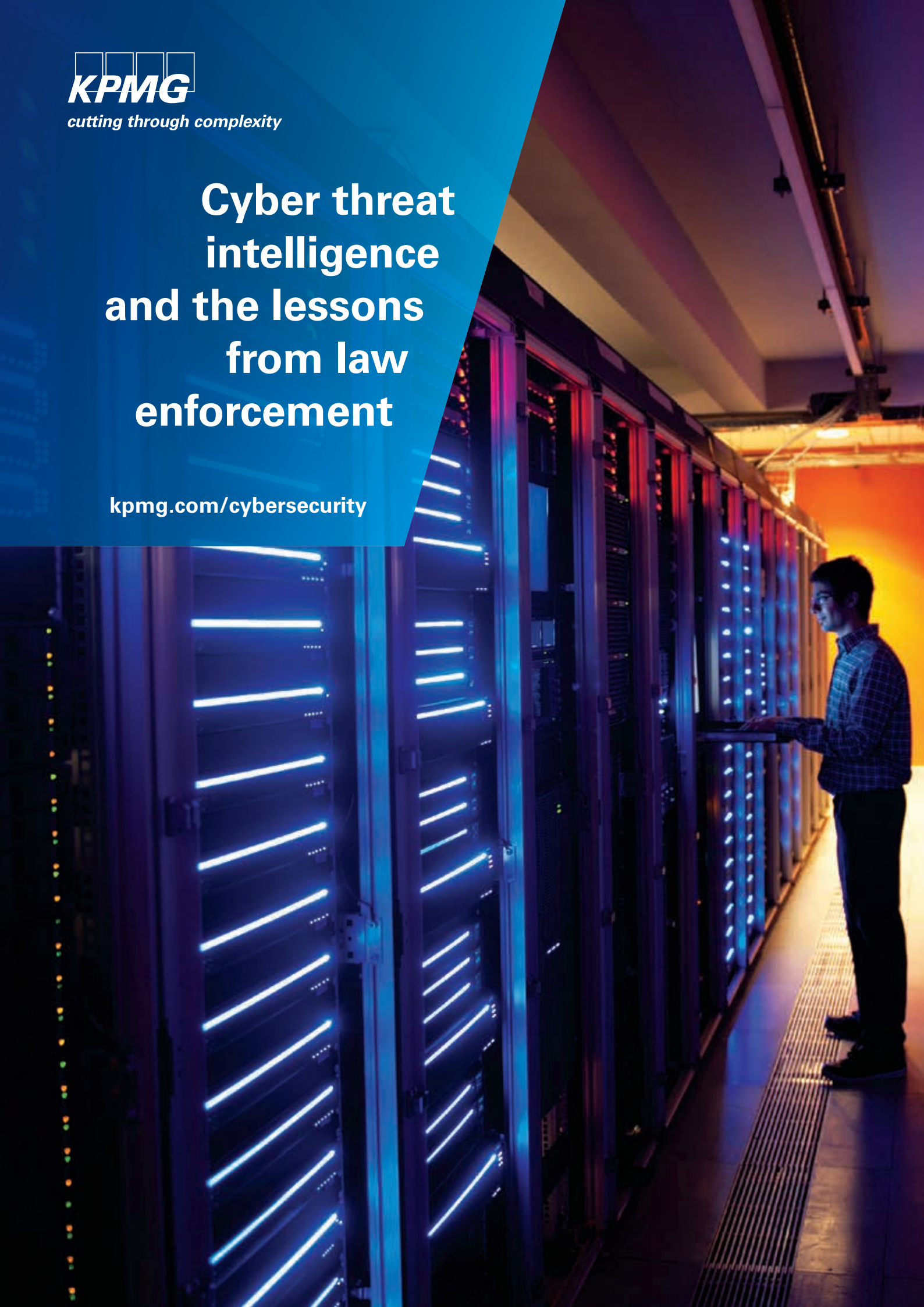
KPMG

cutting through complexity

Cyber threat intelligence and the lessons from law enforcement

kpmg.com/cybersecurity



Introduction

Cyber security breaches are rarely out of the media's eye. As adversary sophistication increases, many organizations react when it is too late – the attack is underway. Few organizations have the capability to anticipate cyber threats and implement preventative strategies, despite prevention being more cost effective[1] and customer focused.[2]

[1] For example: http://money.cnn.com/2012/12/13/technology/security/bank-cyberattack-blitzkrieg/index.html

[2] UK Cyber Crime Strategy, March 2010

This is not a new threat and hackers have been infiltrating sensitive government systems since the early 1990s. However, the focus on cyber security is increasing rapidly due to many high profile and highly disruptive/damaging security breaches threatening financial and physical damage across critical national and corporate infrastructures. It also appears the nature of the threat is changing. In our most recent survey, 67 percent of data loss resulted from external hacking, while the insider threat is surprisingly at an all time low.[3]

The Information Security landscape is constantly evolving. Private and public sector organizations find it difficult to believe they could be a target for cyber attacks. This mindset needs to change – as the best offence is a good defense. At the same time, it is no longer viable to rely on defense. The determined adversary will get through eventually. As a result, organizations must know what is going on around them so that they can identify when an attack has taken place or when an attack is imminent. Intelligence and the insight that it brings is at the heart of next generation Information Security.

An intelligence capability enables organizations to identify potential threats and vulnerabilities in order to minimize the 'threat attack window' and limit the amount of time an adversary gains access to the network before they are discovered. Organizations that take this approach understand that threat intelligence is the 'mechanism' that drives cyber security investment and operational risk management.

The number of cyber threat intelligence providers is on the rise and the concept of threat intelligence is now pervasive. While increased awareness of the cyber security threat is a positive trend, our experience indicates that many organizations now need to focus on putting in place the fundamentals of intelligence management to gain real value from threat intelligence. This will be a pre-requisite for instilling confidence in board members –and ensure that the organizations are equipped to meet the ever-evolving challenges of cyber security.

Much can be learned from law enforcement and intelligence organizations. They have long recognized that intelligence-led decision making sits at the heart of their organizational culture and operations.

KPMG member firms have been privileged to have worked extensively with law enforcement and gain understanding and experience of intelligence best practices along with the common pitfalls.

We believe in three principles that will help organizations manage the cyber threat proactively and minimize the risk to customers, shareholders and employees. These are:

- Create an intelligence-led mindset
- Implement an intelligence operating model
- Build an intelligence-led decision-making process

[3] KPMG Data Loss Barometer, 2012

Principle 1 – Create an intelligence-led mindset
An intelligence-led mindset establishes a direct connection between threat, vulnerability, compliance, risk, action and consequence. It requires leaders to ask simple but fundamental questions on a continual basis. These include:

- What cyber threats do we face?
- What risk do they pose to our valuable information assets?
- What should our response be?
- How effective has our response been?

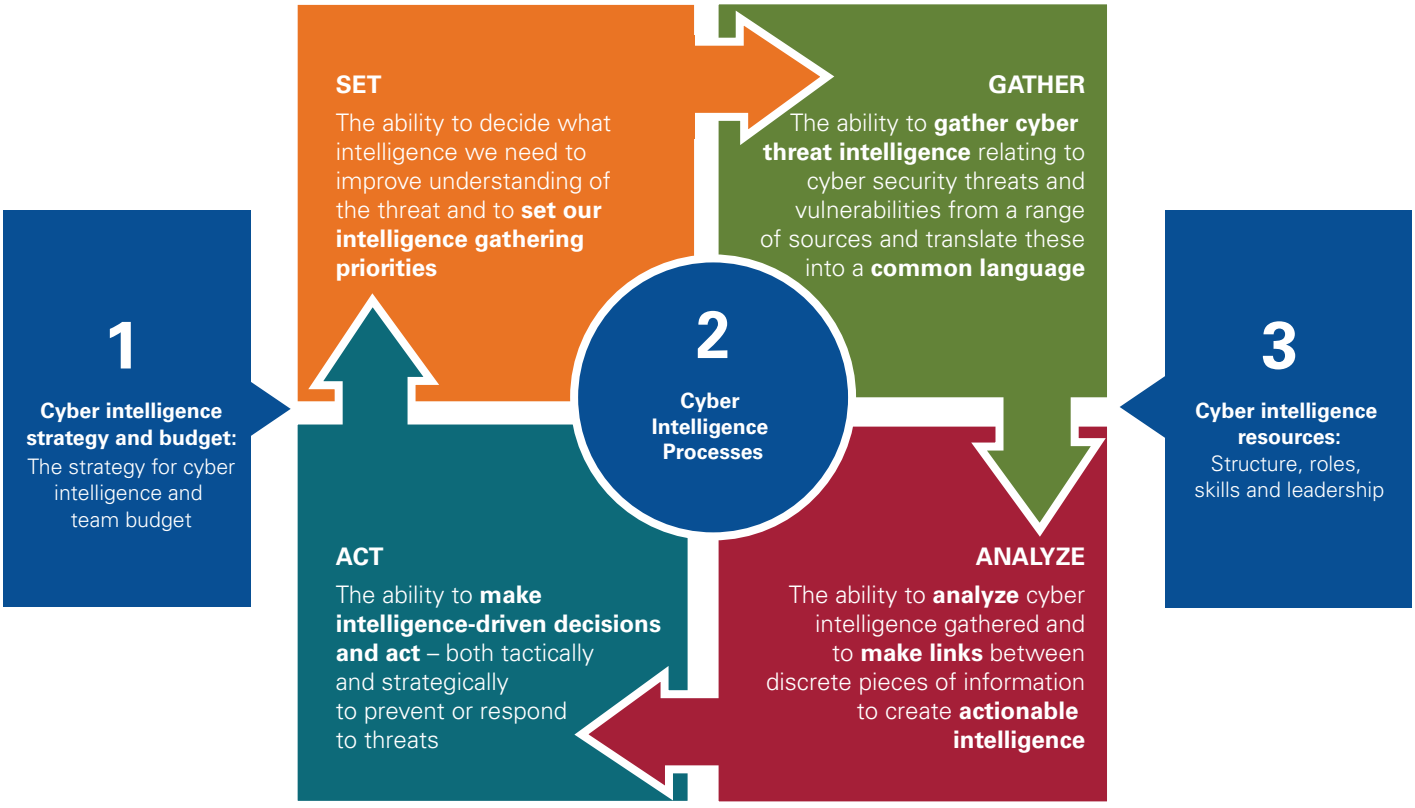
Despite the increasing cyber threat risks, many boards fail to ask these questions or attain satisfactory answers. Often, this happens because the first question is the most difficult to answer. Cyber threats are hard to quantify in terms of likelihood and business impact. Much 'intelligence' is often situational awareness, describing the symptoms or effects of the attack rather than the factual information about the adversary.

As a result, many boards do not fully understand the nature of the threat and, inaccurately assume that cyber security is a technical issue. Management of cyber security is generally confined to the IT practitioners, who are often unable to pull the enterprise-wide levers that are required to reduce risk across the organization.

Adopting a preventative approach requires a cultural shift that starts with board level executives. Focusing on these questions at the board level and incorporating them into the enterprise risk strategy is critical. By doing so, leaders can quickly start to identify gaps in the current cyber security strategy and encourage an organization-wide approach to countering cyber threats.

Principle 2 – Implement an intelligence operating model
To embed an intelligence-led decision-making process into an organization, a basic intelligence model must be in place. Law enforcement organizations use robust systems and processes to collect, analyze and act on intelligence. While these models may vary, they are built on common components that are directly applicable to any organization seeking to develop an intelligence capability.

Our basic intelligence operating model, shown here, is based on our experience of improving intelligence management systems and processes in law enforcement. This paper primarily focuses on the processes that form the basic infrastructure (Element 2).



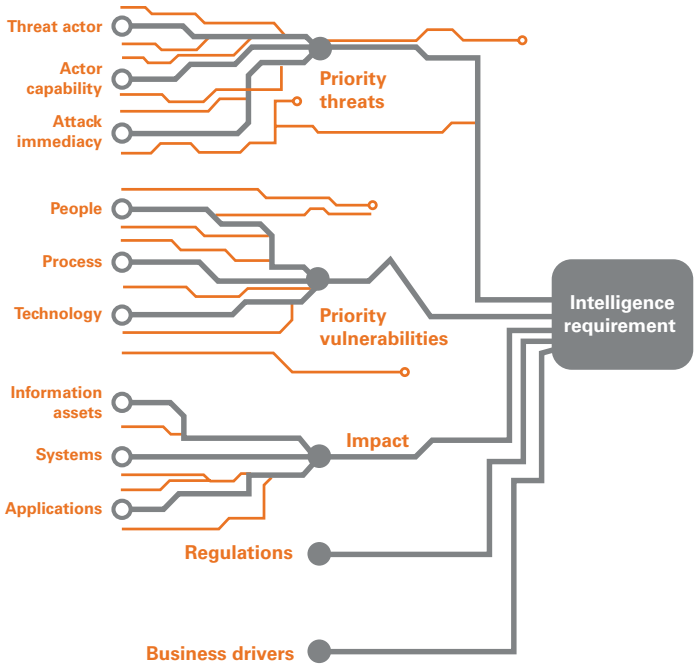
Source: KPMG International, 2013

Setting the intelligence requirement

No organization can dedicate resources to counter every threat. In law enforcement agencies, threats are prioritized and resources are allocated on a priority basis.

Cyber threats are no different and forward thinking organizations are starting to adopt industry frameworks for categorizing them. Similarly, it is possible to identify vulnerabilities and the potential impact of information loss. Intelligence collection should be informed by an understanding of priority assets, possible threats and vulnerabilities.

Just as law enforcement agencies use intelligence to protect the public, organizations should be doing the same to protect information assets, customer data and, ultimately, shareholder value.



Gathering relevant information

>> It is only through collaboration that information can be gathered together and bring into focus the different dimensions of the problem.<<

Gathering relevant information is the first step toward generating actionable intelligence. This activity represents the largest proportion of budget because of the effort and expense of collecting information from diverse sources. Obtaining information about cyber adversaries is a challenge due to the global nature of the threat and the inability of many organizations to exploit useful information that often resides in their own systems. For example, data that may reveal adversary tools, techniques and procedures.

The complex nature of the security threats makes it difficult to see the complete picture. It is only through collaboration that information can be gathered together and bring into focus the different dimensions of the problem.

Establishing effective collaboration is a major challenge. Many organizations are wary of sharing information that could reflect negatively on their brand. Others are distrustful of law enforcement agencies handling their sensitive commercial data. Overcoming this challenge is essential to keep pace with the evolving threat.

Analyzing information to create intelligence

>> Although this may sound simple, many organizations do not properly store and, subsequently, interrogate information relevant to cyber threats. <<

Once information has been gathered, a systematic analytical approach is critical. Three hallmarks of this approach are highlighted here.

1. The ability to search and cross-reference data across multiple systems. Although this may sound simple, many organizations do not properly store and, subsequently, interrogate information relevant to cyber threats. Although the cost of storage may act as a heavy argument for not doing so, the real reason is often a lack of understanding of what to look for.

Mature organizations are increasingly considering the use of analytical tools that seek to identify potential threats by monitoring activity across systems to spot patterns, trends and suspicious activity.

2. Using analytical frameworks to build threat profiles. Many law enforcement and intelligence organizations analyze information from the viewpoints of victims, property, locations, offenders and time. These can be applied directly to cyber threats in the following manner:

Offender: What do you know about the people/organizations responsible for the attacks and what is their modus operandi? Addressing the offender profile is pivotal and should drive all subsequent analysis.

Victim: Is there anything about your business operations that makes you a target for cyber attack? Are certain business units being attacked or more likely to be a target than others?

Property: What information assets are you trying to protect and what is the perceived risk to the security of each asset?

Location: Where (physically and virtually) are the information assets you wish to protect held? What is the current form of protection? Are there any specific servers that are being attacked?

Time: Are there any temporal patterns regarding cyber attacks and, similarly, are your information assets more vulnerable at certain times?

3. Intelligence products or reports must be tailored to the needs of customers. This requires a mature and continuous dialogue to understand customer requirements and to regularly review the quality and relevance of the intelligence products.

Best practice, often used by law enforcement and intelligence organizations, indicates that a dynamic and flexible process of incorporating evolving requirements and responding to immediate needs is critical. At the same time, the intelligence function needs to drive process efficiency and ensure automation. This is particularly relevant for intelligence 'feeds' that are directed to multiple customers in real time.

Acting on intelligence

The best test of the value of the intelligence product is whether it directly informs decisions about how to tackle cyber security risks. For law enforcement and corporate organizations alike the key decisions are as follows:

- When to act?
- Which tactical option to pursue?
- Has it been effective?

These questions are very relevant for organizations that are seeking to take offensive action against the cyber adversary. During an attack, a natural tension occurs between monitoring the attack to gain further intelligence about the adversary versus neutralizing the threat and minimizing loss. This is clearly a matter of judgement; mature organizations often use decoys to induce adversaries to reveal additional intelligence.

Principle 3 – Build an intelligence-led decision-making process

In law enforcement and intelligence organizations, intelligence directly informs all core business decisions. It is evident that corporate boards do not follow this approach consistently. Boards, therefore, might not have a clear view on cyber threats that could have a material impact on critical business decisions.

The London 2012 National Olympics Co-ordination Center (NOCC) is a good example of a mature intelligence capability that was integrated into the governance and decision making structures of the UK policing.

At the NOCC, twice daily tasking and co-ordination meetings set the direction for each day. This meeting cycle enabled senior officers to continually review the latest intelligence picture and allocate resources to mitigate emerging threats. The key learning takeaway is to embed the use of intelligence into core business by aligning the development of intelligence products to the tempo of formal decision making .

Visible seniority is also important. Intelligence meetings at the NOCC were chaired by senior law enforcement officers with the authority (delegated if required) to make dynamic resourcing decisions.

While it may not require this regularity, board level awareness of emerging cyber threats and direct involvement in determining the response is critical. In the uncertain world of cyber security, threat intelligence will help organizations become more proactive, focused and preventative.

KPMG and Cyber Security

KPMG's member firms have designed and implemented intelligence capabilities in law enforcement and intelligence agencies. We also work with some of the world's largest corporations to design their cyber security programs.

This insight provides the team with a unique viewpoint on the building blocks of an effective cyber intelligence function.

We see threat intelligence as the central component to effective cyber security. KPMG member firms help clients design the right model, and embed it into their organizations. The goal is to help member firm clients build a sustainable cyber security capability.

KPMG's Cyber Security Services bring together specialists in information protection and business continuity, risk management, privacy, organizational design, behavioral change and intelligence management. These combined skills are utilized to tailor a strategy relevant to the clients' risk appetite and the cyber threats their organization faces.

KPMG member firms are:

- **Global –** through our member firm network, KPMG employs over 152,000 professionals in 156 countries. We have deep expertise wherever you operate.
- **Award-winning –** KPMG in the UK was awarded 'Information Security Consultant of the Year' at both the 2011 and 2012 SC Magazine Europe Awards. In addition, KPMG's Information Security consulting services capability was named a "Leader" in the Forrester Research, Inc. report, The Forrester Wave™: Information Security Consulting Services, Q1 2013. Of the 10 firms evaluated for this report, KPMG was specifically recognized for its drive to take on the toughest consultancy tasks, often taking over from other firms.
- **Shaping the cyber agenda –** Through I-4, KPMG's Cyber Security Services practice helps the world's leading organizations to work together to solve today's and tomorrow's biggest security challenges.
- **Committed to you –** Relationships with member firm clients are built on mutual trust and long-term commitment to providing effective and efficient solutions. KPMG practitioners are dedicated to providing a service that is second to none.

Contact us

For information on KPMG's services, our cyber security model or to discuss the content of this article further please contact:

Malcolm Marshall
Global Head
Information Protection
& Business Resilience
KPMG in the UK
E: malcolm.marshall@kpmg.co.uk
T: +44 20 73115456

Tony Buffomante
Americas Lead Partner –
Cyber Threat Intelligence
KPMG in the US
E: abuffomante@kpmg.com
T: +1 312 665 1748

Nicholas Fox
EMA & ASPAC Lead Partner –
CyberThreat Intelligence
KPMG in the UK
E: nicholas.fox@kpmg.co.uk
T: +44 20 73115046

Richard Krishnan
Justice & Security
Global Center of Excellence
KPMG in the UK
E: richard.krishnan@kpmg.co.uk
T: +44 0 7770494840

John Hermans
Cyber Security Lead Partner
KPMG in the Netherlands
E: hermans.john@kpmg.nl
T: +31 6 51366389

Visit us at:
www.kpmg.com/cybersecurity

kpmg.com/socialmedia

Designed by Evalueserve.

Publication name: Cyber threat intelligence and the lessons from law enforcement. Publication number: 121412. Publication date: May 2013