Deloitte.

Cyber intelligence today: Proactive and predictive

IT leaders and business executives need to understand how the critical discipline of cyber intelligence is evolving.

Individual cyber intelligence capabilities have been applied for decades, some since the earliest days of IT system design. Beyond the inflection point of a unified, comprehensive approach, there have been significant advancements in the overall discipline. Given the importance of cyber intelligence in today's environment, business executives should join their IT colleagues in understanding how this discipline is evolving. Here's a look at four critical topics:

Cyber security. Many cyber security efforts were geared to detecting and protecting against intrusions of the perimeter. As threats shifted to inside the trust zone (e.g., employees who inadvertently enable security breaches), new tools and techniques were needed. Identity and access management solutions were siloed systems – with isolated entitlements, activity logging, and controls. Pattern detection of higher-order threats was extremely difficult because these solutions had limited access to the context of external events. Technology solutions were manually operated, which the business perceived as a nuisance and often circumvented. The chief security officer (CSO) or chief information security officer (CISO), if they existed at all, were typically technologists with deep domain knowledge, but without a seat in the boardroom.

Today, cyber security is increasingly framed as a combination of architecture, practices, and processes – with equal focus on internal and external threats. Highly integrated tool sets and investments in cyber analytics have helped connect dots and identify previously undetectable exposures. Automated identity management tools are incorporated into day-to-day tasks, including smart cards, biometrics, fingerprint, and handprint scanners. The CSO role has become commonplace, requiring a mix of technology and leadership skills and gaining a seat at the boardroom table.

Cyber forensics. In the past, incident investigations would conclude once a root-cause analysis was completed. These self-contained analyses were rarely used to augment existing controls or update policies. At best, a script was created to improve response in case a breach recurred. Cyber forensics now looks beyond the host to the network layer, determining the source (inside or outside the organization) of the malware. This determination is correlated with other internal and known external threats using cyber analytics, in an attempt to identify future vulnerabilities. Forensics results are part of a closed-loop cycle in cyber intelligence, improving directly affected and associated controls.

Cyber analytics. In the past, cyber analytics was a reactive approach based on situational awareness and descriptive analysis. It provided an understanding of the value of business analytics, but without the models to apply the patterns.

These days, this discipline is an established tradecraft of analytics, reinforced by the realization that threats and opportunities are often hidden in plain sight. Cyber analytics is predictive, prescriptive, and a part of a closed- loop cycle of continuous refinement based on other cyber intelligence activities.

Cyber logistics. Supplier security reviews were typically limited to deal signings and cursory annual audits. Notably in manufacturing, companies relied on several ever- changing sub-contractors and small hardware providers, each with its own risk profile, which created potential weaknesses upstream in the supply chain. Personnel checks occurred only during the hiring or contracting process, with clearance processing handled by largely unknown third parties.

IT risks and security challenges, a Deloitte perspective as published in the WSJ, CIO Journal

Today, cyber logistics includes extensive analysis to identify, assess, and mitigate risks posed by vendors subject to foreign ownership, control or influence, or other significant concerns prior to a purchase or the awarding of a contract. It entails the continuous assessment of suppliers, including organization structures and corporate activity (e.g., M&A transactions) as well as ongoing confirmation of the integrity of goods. Cyber intelligence strategies include provisions for personnel security such as verifying the legitimacy of background investigation agencies, proactive foreign travel risk advisory, and automated reinvestigations of executives and privileged roles.

Going forward, organizations should embrace security and privacy as foundational to their business. Cyber intelligence efforts should be viewed as critical by the C-suite funded as a strategic priority, and empowered to become part of the company's operational DNA.

March 29, 2012, Ted DeZabala
Center for Security & Privacy Solutions

Contacts

James Nunn-Price
+44 20 7303 8708
jnunnprice@deloitte.co.uk

Dean Atkinson
+44 20 7007 5349
deatkinson@deloitte.co.uk

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.co.uk/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte LLP is the United Kingdom member firm of DTTL.

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte LLP would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte LLP accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

© 2013 Deloitte LLP. All rights reserved.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3BZ, United Kingdom. Tel: +44 (0) 20 7936 3000 Fax: +44 (0) 20 7583 1198.

Designed and produced by The Creative Studio at Deloitte, London. 24346A