Three Ways To Re-imagine The Role Of Global Security Teams

Elena Kvochko(Barclays Bank), Troels Oerting (Barclays Bank)

Cyber attacks remain a fast growing business, despite investments organizations make in their cyber defense. Significant drivers for it are increasing sophistication of the threat, prioritization of openness and functionality over security, and a lack of relevant tools on premises of many companies. What is often overlooked, however, but remains important, is a lack of holistic management approaches and organizational silos. Security models have grown organically over many years, but haven't been significantly adjusted to the changing realities.

In the past, organizational security focus was on physical security to protect against attackers operating in close geographical proximity. Companies stored their assets in safes and focused on enhancing physical 'locks on doors'. During the first, second and third Industrial Revolutions, global companies tried to adapt to the development of crime in a multinational context, where the threat changed from being local to regional, then to national, and finally, to international. In the so-called the fourth Industrial Revolution, global companies are facing a much different threat and operate differently. Physical locks to protect assets became irrelevant. Technology brought progress and scale of businesses; institutions are able to serve more clients faster from anywhere at a lower cost. Our neighborhood is not a local district, but the entire globe. The perpetrators of attacks are no longer within miles of reach, but rather in unknown locations, where they may appear unreachable – behind proxies and encryption, with no need to travel. Modern crime is low risk and brings high returns. Technology gave rise to crime-as-a-service.

Consequentially, almost all attacks against institutions now have a 'cyber dimension', in which technology is used as an outright attack vector to obtain money, information, or deface an institution. Financial crime is closely related to cyber crime.

The ecosystem surrounding an institution is composed, among others, of employees and all stakeholders, physical locations, on premise and cloud

infrastructure, third-party providers. All of these components work in parallel towards a common goal, but are independent from each other. In addition, many business units are also structurally isolated from one another. Security models for many large global organizations should account for often disjointed nature of the technology infrastructure, business units within the organizations and have a holistic approach to better detect, react, and recover from sophisticated security threats. These models should be able to coordinate with reporting lines, enable real-time sharing of information, and 'corporate memory' with the ability to recognize patters across channels, products, entities, and lines of business.

To address this, in our view, information security should be integrated with physical security and financial crime divisions in global companies in order to see crime in a holistically way. There is a need to establish an intelligence-led defense resting on adequate cyber hygiene, physical and cyber security controls, with the ability to detect and react to the right 'signals'. In our view, companies should focus not on notions, such as 'Information', 'cyber', or 'physical' describing security, but simply focus on the core: to deliver Security.

1. Streamlining internal security operations

In order to ensure effective defense, cyber security programs should be run on common datasets and work alongside law enforcement entities, based on global acceptable standards with respect for data protection and privacy. Given that products will be delivered online, security, safety, privacy, and trust should be enhanced ensuring that all available information/intelligence are analyzed. Trust and security are at the center of competitive differentiators, since the biggest loss that a company can incur is failure to uphold the implicit agreement with its shareholders, customers, regulators and other stakeholders to keep their sensitive or valuable digital assets safe, thus undermining their trust.

2. Focusing on all types of threats to enable rapid reaction

Security teams should support prevention and mitigation of crimes regardless of its nature – cybercrime, physical crime, information leaks, internal threats – or their detection methods. This "one-stop-shop" could gather intelligence, forensic evidence, help investigate and recover financial losses. It should also make sure that any new modus operandi – any new tools and techniques – are exchanged with the appropriate partners (inside and outside the company, as appropriate)

to enhance cyber hygiene and resilience. Internal policies to face the new threats and risks should be updated accordingly.

3. Restructuring the Internet-facing infrastructure and ensuring specialist analysis and remediation of threats

Coordinated 24/7 intelligence, investigation, and rapid reaction security team working side by side would lead to reduction in losses and costs and improve security. Initial steps should be oriented towards:

• enabling holistic pattern recognition to distinguish between “normal behavior” and “abnormal behavior” to accurately detect suspicious behavior

• allowing cross-channel visibility to detect complex patterns of behavior that may involve multiple layers across channels, products and accounts

• establishing an alert management system to automate decisions and score risk before the investigation process and establishment of a central case management is initiated

• creating the ability to link complex cases in which threats are detected locally within a business line but are part of a global threat that targets several business lines.

By integrating the duplicative functions, building security operations centers, and by focusing on all aspects of Security – People, Processes, Technology – companies can direct, monitor and control the implementation of Security and Trust as a whole. This way they can uphold maximum security for fewer investments.