WHITE PAPER

FireEye®

Evolving Role of Government in Cyber Security

So far, the 21st century has been an era of wide-scale deregulation and privatisation, with much of the nation's critical infrastructure — in sectors such as energy, transport, finance and medicine — now in the hands of the private sector. Adversaries constantly target these critical infrastructure sectors, with security threats potentially causing both cascading and crippling effects regionally, nationally, and even internationally, as a result of the increased interconnectedness and interdependency in our society.

The difficulty in securing critical infrastructures is partly due to the divergence of interests between the private and public sectors. The private sector's primary focus is corporate efficiency: the main goal is profit making, so it implements the minimum level of security needed to achieve profit as quickly as possible. In contrast, the government is principally concerned with achieving social order, national security and economic prosperity for its population. Most developed nations have an **"all hazards"** approach to address a wide range of threats to their populations, yet governments, in some cases, are not the primary security provider. For instance, governments do not always provide close supervision of, or operational control over, the critical infrastructures within the private sector.

Governments are grappling with the challenge of determining what their roles in cyber security could or should be, particularly with regard to the private sector. However, the changing global landscape should not mean that the role of governments as legitimate providers of security be diminished; governments should work to understand how the world has changed and is changing, and what their role(s) should be within this new environment of increasing interconnectedness and interdependency. For governments to be successful in this new environment, their remit must transcend their historical regulatory role. They must now tackle how they can best assist the private sector to invest in security (facilitation), and how public and private sectors can work together to improve the current state of security (collaboration). FireEye proposes implementation of the Regulate, Facilitate, Collaborate (RFC) framework through which governments must strategise and be ready to draw upon analogous lessons learned from past strategies geared towards other threats, such as pandemics and terrorism.

Private Sector Security Investment Decision

Risk management textbooks typically spell out an objective and easy-to-understand equation that describes risk. Put simply, security risk is a function of the:

Likelihood of being targeted

Vulnerability of the organisation

Impact of a security incident.

Risk = Likelihood of being targeted X Vulnerability of the organisation X Impact of security incident

It is logical to assume that, given the high frequency and severity of cyber security incidents — which translates to high security risk — reported almost on a daily basis, companies, especially in the areas of critical infrastructure, are stepping up their cyber security investment accordingly. However, security vulnerabilities with critical infrastructure are on the rise, and it appears that critical infrastructure companies may struggle to invest sufficiently to stay ahead of the rising threats.

Cyber security risk is just one of many competing risk factors companies must take into account in their risk mitigation plan. Some companies simply don't have an appropriate security culture that involves everyone from the CEO to lowest ranking employees to do their part to protect the company from security intrusion. Not having the right security culture creates a negative impact on the security budget, which affects the tools and security savvy individuals that need to be employed. A lack of security investment can sometimes be attributed to companies not having good examples to emulate, but there is also an argument that because the adversaries are so skilful, increased security investment may not be of much use in the long term.

What governments can do is identify the different factors that influence how the private sector makes security investment decisions, and use a combination of tools within the RFC framework to prompt increased security investment.

Market Forces

When companies experience a security incident market forces can cause severe repercussions, including loss of market capitalisation, revenue and profit, brand reputation and market share. With respect to the risk equation, market forces affect the impact variable, and thereby increase the security risk considerably. Companies that believe they will be severely impacted by market forces tend to take security investment seriously. For example, many companies understand the importance of security to both themselves and to customers. As a result, they have made significant investments in key security initiatives, such as supply chain security,[1] Security Development Lifecycle[2] and trust programmes to harden equipment.

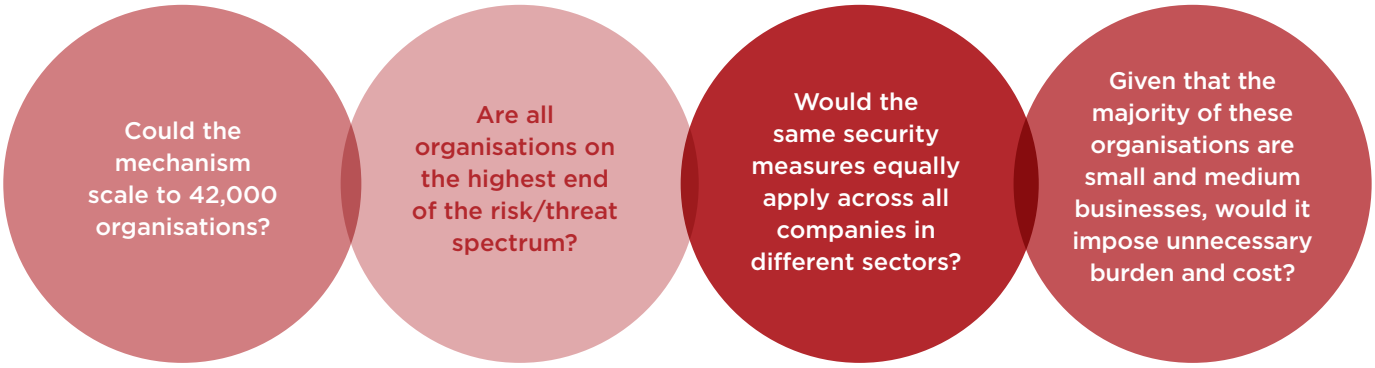
However, not all companies are affected by the same market forces. Non-public listed companies or companies whose products are embedded in bigger systems usually sold by larger companies very often lack incentive to invest in security. Governments need to better understand the factors holding them back and determine what can be done to ensure they step up security investment.

1 https://www.microsoft.com/itshowcase/Article/Content/991/Securing-the-supply-chain-with-riskbased-assessments
2 https://www.microsoft.com/en-us/sdl/

Tragedy of the Commons

The tragedy of the commons was first brought to attention in 1833 by William Forster Lloyd to illustrate the deterioration that would occur in a pasture due to the innate traits of humans. These principles can be extended to cyber security. Companies, especially those with low profit margins, are extremely cost-conscious. If a company's competitors are not making the same level of security investment, the company will be at a cost disadvantage, putting their survivability at risk. Furthermore, when one of their peers suffers from a security incident everyone is impacted by the consequences. For example: in the aftermath of a security incident, the government intervenes by imposing new regulations or security standards that companies must adhere to, thereby escalating the costs for companies who are already making security investment.

Ideally, all companies should be equipped with an equivalent level of cyber security. One way of achieving this would be for governments to impose regulations on all companies, ensuring their compliance with a minimum standard of security. However, regulations should not be viewed as a cure-all solution, because they can be counterproductive when not implemented properly. For example, the European Commission's proposed Network and Information Security (NIS) directive, as part of the EU's cyber security strategy, is aimed at tackling network and information security incidents and risks across the EU. Elements of the directive would require organisations to adopt risk management practices and report major security incidents on their core services. Organisations subject to the directive would include member states, key Internet enablers and critical infrastructure operators, totalling 42,000 organisations. On the surface, reporting major security incidents may seem a reasonable approach, but closer examination reveals potential issues:



Another potential issue with reporting security incidents is it could distract security professionals with compliance requirements and post-attack reputation management, hindering their ability to prevent cyber attacks and mitigate their effects. A further complication is that certain sectors such as finance and banking are already required, by their individual governments, to comply with incident report obligations; additional directives would introduce overlapping requirements. Fortunately in late 2015 the European Parliament decided that only critical infrastructure falls within the scope of the directive,[3] which will allow the European Commission to provide proper oversight and enforcement of a significantly reduced number of organisations.

However, the question still remains: What can be done to reinforce security investment for organisations not covered by the NIS Directive? It is reasonable to assume that some of those organisations are ecosystem partners to critical infrastructure organisations. In an interdependent world, security is only as strong as the weakest link. Lessons might be learned from the Customs-Trade Partnership Against Terrorism (C-TPAT) programme which influences business ecosystems and supply chains.

3 European Parliament (July 12, 2015). MEPS close deal with Council on first ever EU rules on cybersecurity.

Tipping Over the Lead Dog

According to James F. Moore, in a Harvard Business Review article, "Predators and Prey: A New Ecology of Competition",[4] innovative businesses don't evolve in a vacuum because they must attract resources of all sorts, drawing in capital, partners, suppliers, and customers to create cooperative networks. In his view, companies are part of a business ecosystem where they work cooperatively and competitively to support new products, satisfy customer needs and eventually incorporate the next round of innovation. Over time, they coevolve their capabilities and they tend to align themselves with the directions set by the ecosystem leader (also known as the lead dog).

Recognising the dynamics of a business ecosystem leader and members paved the way for the success of the Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary supply chain security programme led by U.S. Customs and Border Protection focused on improving the security of private companies' supply chains. In the early stages of this programme the government worked closely with the so-called lead dogs of business ecosystems in four areas: site security, personnel, material movement and process control. After successfully "tipping over" these lead dogs to sign up to the C-TPAT programme, other members of the business ecosystem began to follow suit and they, under the direction of the lead dogs, started to comply with the security requirements. Today, C-TPAT membership boasts some 11,000+ companies.[5] The main lesson here is that governments don't always have the right answer as to what security measures need to be taken by a diverse set of companies in different sectors, but by working with different business ecosystem lead dogs – who have more know-how in their respective areas – to develop security requirements, the lead dogs can then educate the remaining members of their business ecosystem. As such, the government is indirectly able to help solve the tragedy of commons problem by ensuring all companies are at a superior level of protection through strong security partnership with the lead dogs.

Security Interdependency Within A Vertical

When assessing how to best to use the RFC framework to create a conducive environment for security investment, a government should consider whether there is heavy security interdependency within a particular industry vertical. Critical infrastructure, such as air traffic controls and electric transmission grid companies, exhibit such characteristics: the impact of a disruption to one company will affect other companies. In a security interdependent world, risks faced by one company depend not only on its choices but also those of all others. Do companies then have adequate incentives to invest in security against a risk, the severity of which depends on the actions of others? The situation could go in one of two directions for a company: a decreasing trend in security investment if more and more companies are unprotected, or an increasing trend if more and more companies are protected. A government can play a critical role in improving necessary corporate security investment.

Consider this lesson: In 2008, the European Commission issued a directive called 2008/114/EC, for the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.[6] There are a certain number of critical infrastructures in the EU, the disruption or destruction of which would have significant cross-border impact. This may include trans-boundary cross-sector effects resulting from interdependencies between interconnected infrastructures. Member states forwarded suggestions as to what would enhance European prevention of and response to terrorist attacks involving critical infrastructures. In addition, member states were required to build and operationalise Operator Security Plans (OSPs), or equivalent measures, comprising the identification of important assets, a risk assessment and the identification, selection and prioritisation of countermeasures and procedures.[7]

4 James F. Moore (May-June 1993). Predators and Prey: A New Ecology of Competition.

5 Chris Dreibelbis et.al. (October 2008). Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy.

6 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

7 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The directive was a success: member states worked cooperatively to fulfil the requirements.[8] A government can facilitate security improvements by creating a platform that brings important stakeholders together to collaboratively work out appropriate security measures. Stakeholders invest more when they can see that other stakeholders are committed to the process. They all understand the impact of security interdependency and the fact that it is in everyone's interest to invest in security protection. In this instance the governing entity achieved an appropriate balance between the regulatory, facilitative and collaborative elements to promote a positive outcome for everyone.

Another example is the Information Sharing and Analysis Centre (better known as ISAC). ISACs were created as a result of the U.S. Presidential Decision Directive 63 (PDD-63) in 1998, which requested that the public and private sector create a partnership to share information about physical and cyber threats, vulnerabilities and events, in order to help protect the critical infrastructure of the United States. PDD-63 was updated in 2003, with the Homeland Security Presidential Directive (HSPD)-7, to reaffirm the partnership mission.[9]

Today there are ISACs for 14 critical infrastructures,[10] including: financial services, electric, energy and surface transportation. It is not surprising that ISACs are functioning very well, especially in sectors such as financial services where there is heavy security interdependency between different firms. Membership of the FS-ISAC grew from 68 members in 2004 to 6700 members in 2015,[11] so it could be considered a successful model for information sharing and collaboration.

Exposure to Offensive Mindset

Having the proper security culture within an organisation is of paramount importance. Companies with a good security culture have a greater recognition of threats and invest in skilled security personnel who can effectively use security tools to protect the organisation. But what could a government do to encourage the right security culture within an organisation? One solution, which is both intriguing and possibly counterintuitive, is the training programme created by the Idaho National Laboratory in collaboration with Industrial Control Systems-Computer Emergency Response Team (ICS-CERT), under the purview of Department of Homeland Security.[12] The programme trains the people who run ICS — typically used by critical infrastructure such as electrical power stations, oil refineries and water plants — to hack and attack their own systems.[13] Towards the end of the training participants are split into two groups: a large blue team and a smaller red team. The red team's task is to breach the ICS network and wreak havoc in the production system, while the blue team's job is to defend it. The exercise usually results in the red team gaining the upper hand and successfully creating a "disaster" (e.g. the spilling of toxic chemicals).[14]

The training exercise serves several purposes:

It shows critical infrastructure owners that cyber security incidents can have serious consequences, which may result in death and injury to humans and the destruction of property.

Participants understand that ICS networks can be breached when vulnerabilities are discovered and exploited by adversaries. They have to be more vigilant and better informed on vulnerability alerts and advice put out by ICS-CERT.

Participants learn that critical infrastructure operators with an offensive mindset are better able to anticipate the movement of adversaries and therefore improve and increase investment in defenses.

8 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

9 http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1525290507533&uri=CELEX:32008L0114

10 National Council of ISACs.

11 Ray Irving (February 24, 2016). Threat Intelligence Sharing in the Financial Services Sector.

12 Four Thousand Trained to Protect Critical Infrastructure from Cyber Threats (March 17, 2017).

13 Idaho Lab in a Race to Shore Up Critical Infrastructure Systems (October 3, 2011).

14 Ibid

All three of these purposes contribute to building a proper security culture within the organisation. Training does not involve the regulatory element for the government; only the facilitative and collaborative elements are needed to bring about a positive change.

Threat of Regulation

One powerful tool at the government's disposal is the threat of regulation. Regulation often carries the notion of requiring private sector businesses to do certain things or face penalties. When faced with such prospects, companies tend to do whatever they can to avoid regulation. Thus it is not surprising that, when government agencies perform security assessments — which could be in the form of penetration testing — companies are open to scrutiny and as a result are responsive to these assessment findings, and employ proper countermeasures to close security gaps. Such action provides a strong argument for the legitimacy and effectiveness of the private sector's self-regulation.

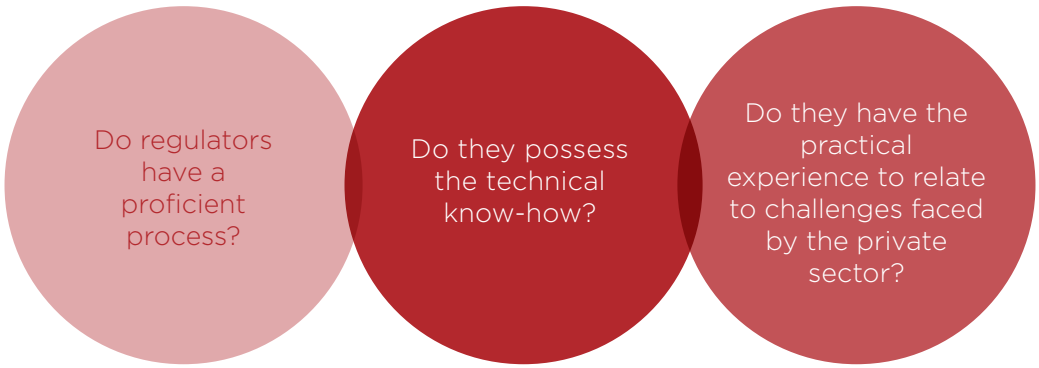
The threat of regulation without the need for a government to impose it could actually avoid potential challenges. In a rapidly evolving cyber security environment, regulation may improve cyber security by making companies address cyber threats of the previous generation but it is rarely equipped to address the constantly changing threats emerging from the current and future generations of technology. Regulation often creates a culture of compliance, and companies often seek the lowest-cost way of meeting these standards. Perhaps such actions would help improve security, but the mindset of compliance-over-security takes away precious private sector resources needed to focus on current and evolving cyber threats.

Trust

Trust is the foundation of successful public-private partnerships.

The trust the private sector places in the government affects whether they accept regulations. Trust provides the lubrication needed to ease inherent frictions between the private sector and regulators. Trust is an expression of confidence between parties, and a low-trust environment makes it much harder for the private sector to accept regulation. It is not uncommon that in a high-trust environment there is acceptance of regulation, even if parties do not entirely agree with a regulatory decision, because they perceive the regulators to be competent, fair and efficient. These three components are the dimensions of trust.

A regulator's competency is the most important component of trust. Many questions help evaluate the competency of regulators:



If the regulators are not seen as competent, additional expertise will be required to establish or reinforce trust. On the subject of fairness, regulators will be evaluated on whether they take everyone's interests into account, not just those of powerful interest groups. Careful management of deliberation is usually required to demonstrate the impartiality of the regulators. The final component, efficiency, is often a sticky point with regulators. It can be perceived to promote bureaucratic red tape, which can then cripple decision-making, complicate the compliance procedure and increase costs. A government should strive to demonstrate that it can process a regulatory decision and the eventual enforcement of the regulation as efficiently as possible.

Risk Transfer

The consensus amongst security professionals is that it is both technically and economically impossible to design and protect critical infrastructure to withstand any and all disruptions, intrusions and attacks. In other words, there is no such thing as perfect security. Logically, then, organisations must manage residual risk. One way to manage risk is to enhance resilience, which enables the organisation to absorb the adverse impact of the security incident and re-establish itself quickly. A complementary method is for companies to utilise the insurance market for risk transfer. However, the cyber insurance market for critical infrastructure is underdeveloped; it is likely that insurers are either reluctant to provide coverage or they charge a high premium, making it too costly for anyone to sign up.[15] From the perspective of the insurers, those concerns may be reasonable.

As addressed previously, cyber security incidents in critical infrastructure organisations could result in catastrophic consequences, such as death and injury to humans and the destruction of property. The impact is often hard to quantify due to a lack of historical data for actuarial analysis. Understandably, insurers are extremely concerned about "black swan" events — low frequency but very high impact — that would make them insolvent. Limited confidence in the accuracy of predictions on the likelihood of successful cyber attacks also exacerbates the matter.

Looking back at the US$40 billion in estimated insured loss that occurred after the events of 9/11, it is clear that the market for terrorism coverage became dysfunctional. Unable to accurately model or price terrorism exposure, insurers and reinsurers withdrew from the market.[16] This resulted in a serious threat to industries in which lenders and investors required terrorism protection for their investments. Subsequently, the U.S. Congress stepped in and passed the Terrorism Risk Insurance Act (TRIA) at the end of 2002, which provided a federal backstop of up to US$100 billion for private insurance claims related to terrorism.[17] The government's role in encouraging and sustaining a properly functioning insurance market is indispensable and the lessons learned from 9/11 could easily be applied to critical infrastructure protection against cyber attacks.

A properly functioning insurance market provides strong incentives for companies to improve their cyber security posture. Insurers, seeking to avoid adverse selection – where they can't distinguish risky organisations – are going to offer insurance premiums and coverage limits that are proportional to the risk faced. Insurers are already partnering with recognised security companies to better understand the risk exposure faced by different organisations. The mere process of applying for cyber insurance can help companies identify tools and best practices they may lack. Insurers may shun companies that have lacklustre security performance; companies with weak security postures will have to invest in security protection to get proper cyber insurance coverage.

15 Insurance Information Institute (August 1, 2016). Background on: Terrorism Risk and Insurance.
16 Congressional Budget Office (January 6, 2015). Federal Reinsurance for Terrorism Risk: An Update.
17 Kevin P. Kalinich, Esq. (January 3, 2017). US Treasury Makes Standalone Cyber Insurance Policies More Valuable.

Conclusion

The case for government to continue to be the legitimate security provider for the nation continues to be compelling. However, governments must strive to understand the changing world of increasing interconnectedness and interdependency to strike a proper balance on how best to use the RFC toolsets to effect a positive outcome for the private sector. Because the security environment around us is complex and different organisations are more receptive to certain measures than others, we must recognise that there is no one-size-fits-all solution. While governments can't control every aspect of cyber security, they can certainly help shape the future of cyber security based on lessons learned from other nations, threats and technologies. Cyber security is vital to a proper functioning and prosperous economy and it is important for citizens to realise the importance of government to the evolution of cyber security in both the public and private sectors.

Learn more about Mandiant consulting services at **www.FireEye.com/services.html**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.
FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye®