WRITTEN STATEMENT FOR THE RECORD OF

STEVE GROBMAN
INTEL FELLOW AND CHIEF TECHNOLOGY OFFICER – INTEL SECURITY GROUP

INTEL CORPORATION

Before the

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON SMALL BUSINESS

FULL COMMITTEE HEARING

On

"SMALL BUSINESS, BIG THREAT: PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS"

APRIL 22, 2015

Good morning Chairman Chabot, Ranking Member Velazquez, and other members of the Committee. Thank you for the opportunity to testify today. I am Steve Grobman, Intel Fellow and Chief Technology Officer for Intel Security Group at Intel Corporation, and I am pleased to address the Committee on the important issue of protecting small businesses from cybersecurity threats. We appreciate the Committee's interest and engagement on this subject.

My testimony will focus on the following areas:

- The threat landscape and its implications for small business
- How best practices and education can help small businesses protect themselves
- How the private sector can deliver security solutions to help small business
- Policy recommendations in support of private sector solutions for small business

First, I would like to provide some background on my experience and Intel's commitment to cybersecurity.

As the chief technology officer for Intel Security Group at Intel Corporation, I set the technical strategy and direction for the company's security business across hardware and software platforms. I joined Intel in 1994 as an architect in IT and have served in a variety of senior technical leadership positions during my Intel career. Before assuming my current role in late 2014, I spent a year as chief technology officer for the Intel Security platform division.

Prior to that role, I spent two years as a chief technology officer at Intel's subsidiary McAfee, where I focused on integrating security technology from the two companies. In prior roles, I served as chief security technologist for the Intel Atom processor system-on-chip design group and spent seven years as chief architect for Intel vPro technology platforms. In the latter position, I led work on the solutions architecture that resulted in a business platform with unique hardware-based management and security capabilities.

INTEL'S COMMITMENT TO CYBERSECURITY

Intel is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices. As a leader in corporate responsibility and sustainability, Intel also manufactures the world's first commercially available "conflict-free" microprocessors.

Security has long been an Intel priority. Indeed, security, along with power-efficient performance and connectivity, comprise the three computing pillars around which Intel concentrates our innovation efforts. A little over a year ago, Intel formed a new business unit to further the security pillar – the Intel Security Group – combining our subsidiary McAfee with other security resources from across Intel to form a single organization focused on accelerating ubiquitous protection against security risks for people, businesses, and governments worldwide.

Intel has long shared the sentiment with the U.S. and global governments that we cannot delay in collectively addressing the evolving cybersecurity threats facing us all, and indeed our company has been at the forefront of efforts to improve cybersecurity across the compute continuum. As a leading developer and manufacturer of foundational information and communications technology products, we offer a unique understanding of the gravity of our cybersecurity challenges, and the reality that governments, businesses and consumers are facing a cybersecurity threat landscape that has changed fundamentally. Countering these increasingly sophisticated threats to all organizations requires the cooperative efforts of government, industry and non-governmental organization (NGO) stakeholders working together to improve cybersecurity in a way that promotes innovation, protects citizens' privacy and civil liberties, and preserves the promise of the Internet as a driver of global economic development and social interaction.

Intel Security delivers proactive and proven solutions, services, threat intelligence and analytics that help secure systems and networks around the world, allowing users to more securely connect to the Internet and browse and shop the web. Fueled by an award-winning research team, Intel Security creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. Last year, we co-founded the Cyber Threat Alliance with other security vendors to drive a coordinated industry effort against cyber adversaries through deep collaboration on threat intelligence and sharing of actionable indicators of compromise, allowing alliance participants to deliver greater security to customers including small businesses.

PUTTING SOLUTIONS IN CONTEXT:
Understanding the Threat Landscape and its Implications for Small Business

Increasing Sophistication of Attackers Threatens Organizations of Every Size. Over the past decade, the attacker type has evolved from recreational "hackers" with limited capabilities to organized crime and state sponsored actors employing extensive resources and highly skilled personnel. At the same time, the stakes for breaches continue to rise.

The attacker community has matured so far that a vibrant criminal underground economy has emerged. Online web stores now sell hacking tools to any would-be attacker, and online markets make it easy and efficient to sell stolen credit card information.

The increasing sophistication of attackers and, hence, attack types, places tremendous pressure on today's security processes, tools and people. These sophisticated attackers are developing new techniques that are substantially more difficult to detect and stop. The most advanced techniques extend beyond exploiting vulnerabilities in the operating system or applications and are now starting to attack the underlying virtual machines, firmware and hardware.

Small and medium sized businesses (SMBs) are just as vulnerable to these same sophisticated cybersecurity threats as large corporations, in both strength and type. While most stakeholders today generally acknowledge that cybersecurity threats are becoming increasingly sophisticated, evolving and intensifying, many in both government and industry nonetheless believe the threat an organization faces is commensurate with its size, essentially assuming that smaller organizations face smaller threats. As recent events such as Operation Source and Heartbleed have demonstrated, however, today SMBs face many of the same threats as large organizations, and experience similar negative consequences. According to Verizon's just-released 2015 Data Breach Investigations Report, while larger organizations post higher losses per breach, further investigation finds that larger organizations just typically lost more records than smaller organizations, and thus had higher overall cost. Breaches with equivalent record loss had similar total cost, independent of organizational size.

Innovative Technologies Bridge Resource Gaps for SMBs, But Also Magnify Threats. It should come as no surprise that cyber criminals follow the latest technology trends because that's where the targets are the most promising. Technological innovations help enable some of the key building blocks to provide better security to SMBs, but at the same time present some of the key security challenges facing SMBs, including:

- *Mobile Threats*: Small businesses, as others, are relying more on mobile devices for not only communication but for business processes, and there's every reason to believe this trend will continue. Malware written specifically to attack mobile devices is also increasing, creating new challenges as the security industry adapts to counter threats to mobile as well as traditional compute platforms.
- *Migration to the Cloud*: Another information technology (IT) trend that serves small business particularly well is migration to the cloud. Small businesses, in particular, can find real efficiencies in outsourcing their IT and communications systems to the cloud. They can reduce costs, improve offerings, eliminate complexity and have less need for onsite IT staff. These are great objectives – as long as security is not sacrificed.
- *IOT and the Explosion in Number of Devices.* Coupled with the above are trends such as the Internet of Things (IOT), which multiply mobile growth beyond phones and tablets, to a wide array of internet protocol (IP) devices that SMBs and others now need to worry about, such as networked metering devices, sensors, appliances, and point of sale systems. While the promise of IOT innovation brings great potential benefits to more offices and businesses across the country every day, it also carries with it new security risks that must be managed.

- *Clients are Often not Connected to Company Networks*: Given the mobile nature of today's workforce, as well as the increasing use of BYOD (bring your own device) programs, users at companies of all sizes commonly access resources from external networks such as hotspots and home networks. The result is that company-owned network equipment is simply unable to inspect a growing percentage of traffic and protect a large swath of users and devices.
- *Traffic is Encrypted*: Even when accessible, application and web traffic is increasingly encrypted. Network security devices are therefore unable to inspect the traffic's content. The coarse-grained information available to network products can provide baseline protection, but is insufficient to detect advanced threats. The shift to "Apps" (such as Android or iPhone Apps) further heightens this challenge, as many of these applications require encryption.
- *Performance Issues Preempt Security*: Customers are turning off security vendors' next generation firewall features such as deep packet inspection (DPI) to maintain network performance levels – creating a tug of war between security and performance priorities.

Adversaries Enjoy Significant Advantages. Understanding the complexity of today's threat landscape demands an examination of the threat actors carrying out the cyber attacks. Our research and analysis reveals that cyber adversaries benefit from and exploit several key advantages, including:

- The ability to *quickly enhance the tools and capabilities of attacks* through a community of innovators and service providers continuously specializing in threats and infrastructure. This attribute creates additional exposure for SMBs, who may not have the resources to deploy the latest adaptive technologies, or are not deploying risk management-based solutions at all.
- A *working knowledge of how organizations implement defenses badly*, including knowledge of specific product deployment models, industry architectures, and even specific organizations' defenses that provide opportunities for attack. SMBs may also be particularly susceptible here, as they may be more likely to deploy "yesterday's" solutions due to resource constraints or other factors.
- The reality that those waging cyber attacks have *unlimited opportunities to learn which tactics are effective* against specific standards and products – thus they only have to be right once. Again, because SMBs are more likely to deploy retail products, including those likely intended for consumers, rather than enterprise-focused solutions, they may be disproportionately impacted here.

Countering such advantages is difficult for even well-resourced security vendors or large corporations to manage; the edge adversaries hold over SMBs is even more pronounced.

The Attractiveness of SMBs as Targets. If we add up the elements of the threat landscape we've covered thus far – the sophisticated threat landscape facing SMBs, the challenges magnified by innovative technology trends, and the advantages enjoyed by potential adversaries – it should come as no surprise that SMBs represent increasingly attractive targets for cyber attacks. Many highly sophisticated and well-resourced attackers perceive that large organizations have deployed greater defense resources and so over time have become harder to breach. In response, they have turned their attention to SMBs as a means to create revenue from a large number of less-protected targets, or as an alternate and easier path to infiltrate large organizations.[1]

This last point is worthy of particular emphasis. Small businesses are not only at risk of high-volume attacks intended to infect as many devices/systems as possible, such as ransomware attacks, but are also at risk of being specifically targeted by adversaries. A primary reason for this is SMBs are attractive as an attack conduit to breach larger business or government targets rich in high-value data or other assets. This concern is not hypothetical. Some of the major breaches in 2014 were originated via SMBs providing facility services to major corporations.

Attacks of this type launched on SMBs can impact numerous industries and vertical markets. While the details of each attack differ, modern attacks share a common pattern with five distinct stages. The full lifecycle of a targeted attack may take months or even years to plan and execute. As an illustrative example, consider the five stages of a recent attack against a retailer that was in part facilitated by an SMB:

- *Reconnaissance*: The goal of reconnaissance is to learn about the organization's employees, IT infrastructure, and other details relevant to launching an attack. A common method for gathering information is through social engineering where an end-user is fooled into surrendering data or undertaking action to compromise his or her environment. In the case of one larger retailer, cyber criminals found vulnerabilities not within the retailer itself, but through a much smaller outside vendor. The attackers used reconnaissance to learn the identity of the retailer's heating, ventilating, and air conditioning (HVAC) vendor and then used email phishing to steal passwords used by employees of that SMB provider.
- *First contact*: Once the attacker finds an entry point, s/he gains initial access to a company's network or endpoints. The retail victim's attackers used the HVAC employee credentials to access the retailer's network. They scanned the network and identified the Point of Sale (POS) terminals.

[1] "Smaller companies are attractive because they tend to have weaker online security. They're also doing more business than ever online via cloud services that don't use strong encryption technology. To a hacker, that translates into reams of sensitive data behind a door with an easy lock to pick." *Why Your Business Might be a Perfect Target for Hackers*, Inc. Magazine, available at: http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html

- *Local execution*: After having infiltrated a network, the next step of an attack is to design and execute code to exploit vulnerabilities on a device. The most dangerous exploits are often sophisticated "zero-day" attacks that uniquely target the victim and have never been seen previously. In the case of this retailer, however, the malware used to infect the point of sale systems were well known.
- *Establish presence*: The next step is to execute code to gain privileges, expand to other systems, and take evasive action to avoid detection. Malware often provides "back door" access to allow full remote control. In this example, the goal was to obtain credit card information. The malware spread to 90% of the company's stores, used a technique to scrape credit card details from the systems' memory, aggregated the information on a staging server, and ultimately transferred it to servers located overseas.
- *Malicious activity*: The final step is to perform the malicious activity, be it destructive or financially motivated. The attacker in this example sold the harvested credit cards on the black market for an estimated $25 to $45 U.S. dollars each.

There were a number of high profile cyberattacks in 2014 impacting hundreds of millions of individuals in the aggregate that followed a similar and a predictable pattern performed by sophisticated adversaries (though not all involved an SMB as an attack vector). Traditional security technologies have proven inadequate in the face of these attacks.

LAYING THE GROUNDWORK FOR SOLUTIONS:
Helping SMBs Help Themselves through Education and Best Practices

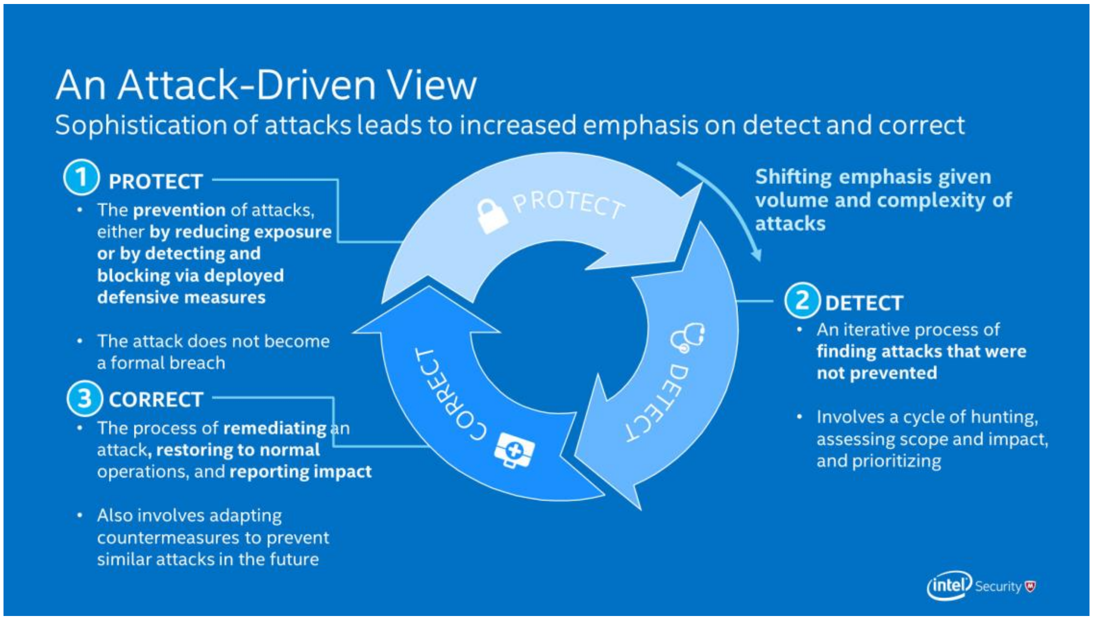
The biggest problems facing SMBs seeking to protect themselves from cyber attacks are often not related to technology. A foundational question is whether they have the resources, know-how and capacity to deploy existing technology solutions efficiently and effectively across their small enterprises. While the reality is today they may not, we offer some suggestions to help lay the groundwork for the more efficient deployment of technologies by SMBs.

Significant education and support of SMBs is needed in order for the promise of technological solutions to be fully realized. This committee has likely heard previously that many SMBs lack the resources to stay current with cybersecurity best practices, and many SMBs may believe that cybersecurity is not an issue or priority for them because of their size. In reality, small businesses store personal information, implement operational requirements and own valuable intellectual property just as large enterprises do, so they too need strong cybersecurity protections. A compelling and focused education system for SMBs is needed to ensure they understand the need for cybersecurity at all organizations, to better and more quickly enable them to determine the best practices to meet their specific risk issues and implement them efficiently. According to the Small Business Administration, SMBs comprise 95% of all U.S. businesses and generate more than half of the nation's gross domestic product. When looked at in the aggregate, budget constraints amongst smaller businesses accentuate the need to drive adoption of connected, ecosystem-based strategies around security planning and investment.

SMB education efforts should be grounded in flexible and nimble risk management based solutions that protect, detect and correct. As discussed above, cybersecurity risk is not only complex but dynamic. Because we face a constantly evolving threat landscape, we must develop best practices to help mitigate those shifting risks. Regardless of their size or resources, SMBs and all organizations must be allowed to prioritize and focus on the most serious risks to the most critical assets, systems, and processes based on their unique business and threat profiles.

The increasing sophistication, volume and complexity of attacks are driving Intel Security and the rest of the security industry to focus more on non-deterministic detection of attacks. This is part of a holistic, risk management based approach that places a proportionate emphasis on protecting systems, detecting the attacks, and a corrective process that involves responding to and remediating attacks so as to restore normal operations.

This three phase construct – protect, detect, correct - encapsulates what I like to refer to as an attack-driven view. (See Figure 1.)



An Attack-Driven View

Sophistication of attacks leads to increased emphasis on detect and correct

1 PROTECT

- The **prevention** of attacks, either **by reducing exposure or by detecting and blocking via deployed defensive measures**
- The attack does not become a formal breach

3 CORRECT

- The process of **remediating** an attack**, restoring to normal** operations, and **reporting impact**
- Also involves adapting countermeasures to prevent similar attacks in the future

Shifting emphasis given volume and complexity of attacks

2 DETECT

- An iterative process of **finding attacks that were not prevented**
- Involves a cycle of hunting, assessing scope and impact, and prioritizing

Figure 1.

Large enterprises are now comprehending the reality of today's threat environment, and are investing resources not only to protect their IT and network assets, but also in the detect and correct pieces of the puzzle. As SMBs are often vendors to large enterprises, those large enterprises need to analyze the threats posed by connecting SMB systems to their greater and extended company IT infrastructures. While SMBs of course need to continue deploying solutions designed to protect their networks, they also need to invest in all three of these fundamental risk management functions. No organization, large or small, is ever going to eliminate threats entirely and successfully block all attacks from penetrating its systems. Cybersecurity spending at any scale must reflect this reality, and adequately apportion resources across all risk management functions.

A useful reference tool for SMBs in prioritizing and managing risks is the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"),[2] which Intel has supported from its inception through its early implementation. President Obama issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity in February 2013 and over the ensuing year Intel collaborated with government and industry stakeholders to help develop the Framework as a flexible risk management tool to improve cybersecurity, grounded in consensus best practices and international standards. The first version of the Framework was delivered on February 12, 2014, and soon thereafter Intel launched a pilot project to test the Framework's use at Intel. Our pilot project assessed cybersecurity risk for our Office and Enterprise infrastructure, and demonstrated that the Framework provided clear benefit to Intel.

We focused on developing a use case that would create a common language and encourage the use of the Framework as a process and risk management tool, rather than as a set of static compliance requirements. Our early experience with the Framework helped us harmonize our risk management technologies and language, improve our visibility into Intel's risk landscape, inform risk tolerance discussions across our company, and enhance our ability to set security priorities, develop budgets, and deploy security solutions. The pilot resulted in a set of reusable tools and best practices for utilizing the Framework to assess infrastructure risk; we plan to use these tools and best practices to expand Intel's use of the Framework. A detailed account of our pilot project and the benefits we derived from using the Framework is contained in the white paper we published in February, *The Cybersecurity Framework in Action: An Intel Use Case*,[3] which we can provide to the Committee upon request.

[2] To read about the Cybersecurity Framework, visit: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. It is worth noting that the five core functions of the NIST Cybersecurity Framework (identify, protect, detect, respond, and recover), are the rough equivalent of and track closely the upleveled, even more simplified protect-detect-correct construct discussed above.

[3] To read Intel's White Paper, *The Cybersecurity Framework in Action,* visit: http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html

Intel encourages other organizations to follow the path we forged by developing their own Framework use cases and driving adoption of the Framework across their ecosystems. Intel recently took the initiative to link the Framework to our Supplier Guidelines,[4] in an effort to make sure our ecosystem of suppliers, including many SMBs, are using sound risk management-based security practices focused on not only protecting, but other important risk management functions such as detecting, response and recovery.

Indeed, the Framework can serve as a foundational educational tool for SMBs, providing a common language for better communicating with security vendors and other business partners, as well as key learnings as to why cybersecurity should be grounded in a risk management approach. Security vendors such as Intel Security can also play a role in helping SMBs help themselves, by developing innovative new solutions and implementing functionality in their products to provide the risk management benefits of the Framework in ways that can be efficiently deployed by smaller enterprises.

DELIVERING SOLUTIONS:
How the Private Sector Can Provide Technology Solutions to Small Businesses

As I testified earlier, often the biggest problems faced by SMBs are not related to the technologies that can help them better protect, detect and correct in the face of cyber attacks.   The primary obstacles to realizing better cybersecurity in SMBs are better characterized in terms of resources, know-how and capacity to deploy existing technology solutions and capabilities efficiently and effectively in a holistic manner.

As mentioned previously, the security industry faces significant challenges to staying ahead of attackers. But security innovation is helping us make progress toward overcoming adversary advantages, better mapping technologies to risk management functions, and providing security connected solutions.

Overcoming Adversary Advantages. Viewed through the lens of a security provider, for our industry to effectively defend against targeted attacks, we must overcome the advantages discussed earlier that tilt the playing field in favor of our adversaries. At a conceptual level, doing so calls for: (1) integrated and collaborative solutions; (2) simple and sustainable architectures; and (3) analytical, active and adaptive environments.

- **Integrated & Collaborative Solutions**. We must counter our adversaries' *innovation and infrastructure advantages* with solutions that enable individual solutions to quickly share what they are seeing (detections, indicators of attack,

[4] To review Intel's Supplier Policies and Framework Guidance, visit: https://supplier.intel.com/static/governance/supplierpolicies.htm

indicators of compromise), and update collective threat detection based on shared information.

- **Simple & Sustainable Architectures**. We must counter our adversaries' *organizational/enterprise knowledge advantages* by allowing organizations to easily and efficiently implement new technologies that reflect changing business requirements and the evolving threat landscape over time. Doing so requires the industry change how we design security technologies, and organizations such as SMBs change how they think about buying, implementing, and managing those solutions. We discuss some of these changes below in the context of our "Security Connected" approach.
- **Analytical, Active & Adaptive Environments**. We must counter our adversaries' *tactical advantages* by forcing them to be right more than once, providing a security environment that analyzes data, recognizes targeted attacks in progress, anticipates their tactics, and takes action to contain and mitigate their impact, while also enabling organizations to recover and adapt their security posture to deflect future attacks.

Mapping Security Capabilities to Risk Management Functions. The Security industry also needs to more fully map critical security capabilities to all phases of risk-management-based solutions, including the protect, detect and correct functions discussed in the preceding section.

Technologies used to defend against the attacks of today can be grouped into three, self-reinforcing, categories:

- *Protect*: Protection is a deterministic approach to stop hackers from infiltrating systems. These technologies protect information from unauthorized modification, destruction or disclosure by reducing the attack surface, encrypting confidential data, authenticating users, defining policies and blocking known attacks. Much of the vendor ecosystem has historically focused on this class of technologies. Many products use "signatures" and other deterministic algorithms for detecting malware.
- *Detect*: With the increased threat environment, even the most sophisticated protection technologies are likely to prove insufficient alone. Timely detection and notification of a compromise become critical. Security teams need more non-deterministic tools to inspect events across their environment to identify malicious activity. Early signs suggest detection is becoming a greater area of focus.
- *Correct*: A system must be recovered to a known-good state following a breach. Security teams address alerts, investigate breaches, complete forensic analysis, remediate damage and restore services. Ultimately, teams implement future

protection safeguards to prevent similar attacks from reoccurring. Scalable and comprehensive correction technologies are only just beginning to emerge.

With the increase in attack volume and sophistication, defenders are naturally shifting their emphasis from a protection-centric approach to one more equally balanced with detection and correction.

Putting It All Together: How a "Security Connected" Approach can help SMBs. In order to do security well, you need integrated solutions, as well as a common mechanism for those solutions to exchange information. At Intel, we refer to this concept as "Security Connected," or the ability of multiple security solutions and products to work together to exchange information. A Security Connected architecture is the primary methodology that Intel Security is investing in to more rapidly detect threats, and we urge the rest of the Security Industry to make similar investments.

Executed correctly, a Security Connected architecture can detect behaviors over time and begin to recognize, almost biologically, threats before they can overtake systems or network functionality. A connected, behavior-based approach enables solutions to communicate observed behavior amongst each other. Security can thus be managed in real-time based on policy that adapts to current threats and provides resilience: the ability to run while under attack. These intelligent systems are the result of innovation, and we need to help small businesses make wise – not expensive – choices to create a connected security foundation.

The below diagram provides a high-level depiction of how the products and systems comprising a Security Connected infrastructure might fit together and communicate in a non-deterministic way.

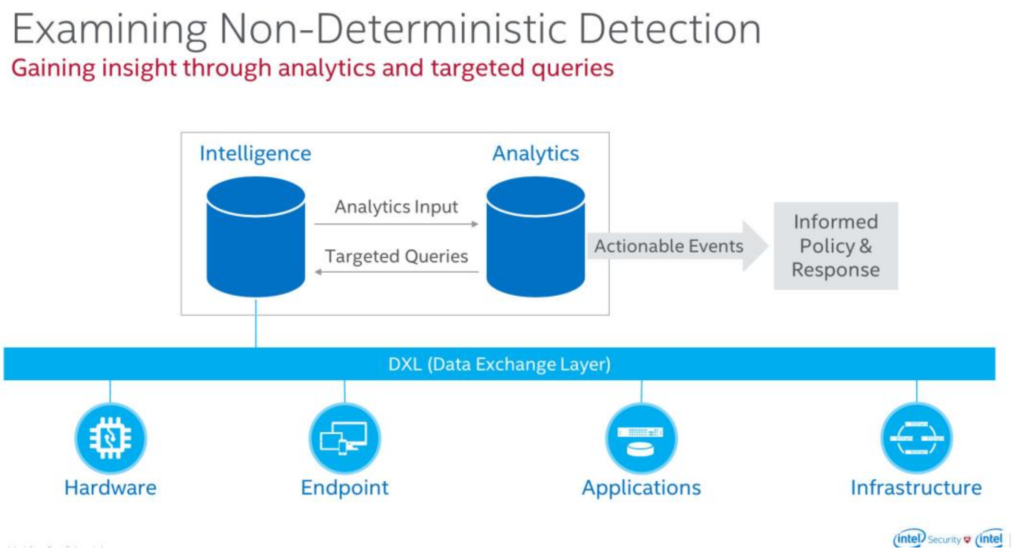

Examining Non-Deterministic Detection
Gaining insight through analytics and targeted queries
Intelligence
Analytics
Analytics Input
Targeted Queries
Actionable Events
Informed Policy & Response
DXL (Data Exchange Layer)
Hardware
Endpoint
Applications
Infrastructure
intel Security intel

Figure 2.

Together, Intel's fully-integrated Security Connected platform embraces a number of security capabilities, though certainly not all organizations are likely to require deployment of all capabilities. Key capabilities represented in the above diagram include:

- **Analytics**, or optimized performance for actionable decision-making
- **Threat Intelligence**, or adaptive intelligence that provides stronger protection
- **Security Management**, or a simplified management experience that reduces effort and cost
- **Context & Orchestration**, or an integrated data exchange that helps deliver cohesive defense

Intel Security is particularly focused on three sustainable advantages that, when delivered together, improve overall security by amplifying the collective capabilities of the many individual solutions referenced above:

- **Messaging layer – Data Exchange Layer (DXL)** provides a standard for classifying and communicating details on attacks between individual product components
- **Centralized inspection – Threat Intelligence Exchange (TIE)** provides a framework for security products to collectively pinpoint threats and act as a unified threat defense system, providing adaptive security resilience and immunity to infections
- **End to end intelligence** – **Global Threat Intelligence (GTI) and local threat intelligence** provide a wealth of information and actionable insights on attacks across all the key attack vectors: file, messaging, network, and mobile.

Consistent with the above concepts, companies like Intel Security can develop world class security capabilities that larger companies with well-funded IT security departments can run as on premise solutions. However, we shouldn't think of SMBs as needing to necessarily acquire and deploy these capabilities directly. In certain SMB scenarios, deploying such solutions on premise may of course make sense. However, it is viable for even the smallest of companies to have access to these very same solutions, even if they do not have the resources to hire an army of IT security professionals, thanks to innovations such as the cloud and the Software as a Service (SaaS) offerings it helps enable. The security industry is able to leverage cloud and SaaS innovations to provide integrated security solutions that deploy increasingly complex technology and are comprised of multiple software and other products, but at the same time essentially mask the underlying complexity from the leanly staffed IT departments at SMBs who deploy them.

The way in which SaaS can help take the complexity out of the equation for small businesses by leveraging the Cloud is perhaps best illustrated by an example. Kenosha is a city in Wisconsin with a limited budget and relatively small IT staff of three protecting a network of approximately 300 work stations distributed across thirteen locations. To meet its security requirements, the city of Kenosha utilizes a cloud-based SaaS integrated solution for Kenosha’s email security and encryption, web security, desktops and file servers, as well as intelligent routing technology. The fact that this type of SaaS security system is utilized across 13 different locations, yet managed by a team of only three IT professionals, demonstrates how cloud based-solutions can be leveraged in lieu of on premise solutions larger organizations have the luxury to deploy.[5]

Security Connected and the Cybersecurity Framework. The Security Industry has begun the process of mapping products and services to the Cybersecurity Framework as part of an effort to help SMBs and other customers bring order to the chaos of seemingly too many products and a lack of knowledge regarding how to use them. Because the Framework was informed by industry inputs and existing best practices, we believe current and future security solutions will map easily and intuitively into the Framework. Doing so should help SMBs better understand what solutions they need – and which to deploy.

Even absent a fully mature mapping to the Cybersecurity Framework, Intel Security’s Security Connected platform unifies and simplifies the management of network and other defenses, while enabling real-time exchange of threat intelligence, analysis, and response that reduces time to detection and mitigation of attacks, and lessens the damage inflicted by them.

The Role of Continued Innovation and Integration. In addition to providing integrated security solutions, the security and IT industries must keep their focus on innovation in order to help small business and other organizations. At Intel, we feel strongly that the path forward is for security to be integrated into products at the beginning, for disparate islands of security to be connected, and for security vendors to offer real-time situational awareness of threats.

We also believe that as a security industry we must unify, simplify, and strengthen the way we provide security. We need to provide frameworks and open standards for integrating potentially disparate technologies – building bridges between security islands to close coverage and technology gaps. This is the rationale for our Security Connected approach. With cybersecurity integration, security companies and their small business customers will be able to more quickly and comprehensively detect and deter threats.

FURTHERING SOLUTIONS:
Recommendations for Policymakers to Further SMB Cybersecurity Efforts

Government can play a vital education and awareness role. As discussed earlier, government can help SMBs by promoting the value of risk management approaches

[5] http://www.mcafee.com/us/case-studies/cs-city-of-kenosha.aspx

such as the Cybersecurity Framework, and all cybersecurity efforts regarding SMBs (educational and otherwise) should acknowledge the high level of threat faced by even the smallest of organizations. The government can additionally help reinforce the value of affordable cyber security solutions to SMBs, filling a vital role in enabling industry to meet the cybersecurity needs of SMBs by raising awareness among vendors and solutions providers of the role SMBs actually play in protecting the nation's critical infrastructure. Doing so will inform and educate industry providers to understand the nature of the threat and foster innovative SMB solutions accordingly.

Don't Forget about the Framework … and be patient. Implementation of the Cybersecurity Framework is still in its infancy, and policymakers should resist the urge to prejudge it. For instance, we understand why government stakeholders are anxious to gain a better understanding of whether the Framework is "working," and that some of those stakeholders will perhaps be less patient than others as we collectively seek to make sense of the extent to which the Framework is gaining traction across industry. It will take some time to see the impact from efforts such as Intel's inclusion of the Framework in our Supplier Guidelines, and in the meantime the government should encourage similar Framework advocacy.

Cybersecurity is a shared responsibility, but industry should lead. Private industry is already conducting a significant amount of work around best practices via consortia and other arrangements, as well as developing and deploying security products, services and other solutions. We do not believe government agencies should play a role in establishing guidelines for security providers, as that is not consistent with the voluntary nature of the Framework, and we note that any policy that may inhibit the market or innovation, or restrict the flow of necessary threat and risk information, could inhibit the marketplace from providing such solutions, impacting the availability of such solutions to SMBs and others.

Leverage lessons learned from small government organizations. State, local, and tribal governments (SLTG) are very similar to SMBs. The very largest SLTG economies draw the most attention and are often the model used when considering all of SLTG. However, the large majority of SLTGs are actually much closer to private SMBs in size and maturity, as suggested by the Kenosha example cited earlier. There are some obvious differences, but consideration of SLTGs should be included in efforts to improve SMB cybersecurity as the risks and solutions will often apply to both.

There is no need to reinvent the wheel—many existing interfaces and solutions within the Small Business Administration (SBA) can be leveraged to help SMBs. Many SMBs already have established relationships with the SBA, and are familiar with the services they provide as well as the procedures used to access them. We urge policymakers and other interested agencies such as DHS to fully partner with and support SBA and its programs when working with the SMB community.

Security mandates on SMBs won't work. Private industry provides a range of products and services at various price points, designed to address the needs of organizations of varying sizes and sophistication. We recognize some SMBs may struggle with limited resources to implement their security plans. However, we believe that it is ultimately up to the organizations themselves, not government, to ensure they have met their own cybersecurity goals, just as it is up to industry to find ways to enable SMBs to more effectively manage their own cybersecurity risks in the marketplace. That is why we advocate for education and support efforts intended to better equip SMBs with the tools to assess and implement their own cybersecurity goals and plans, and for security vendors to develop cost-effective solutions to aid in this effort.

Policymakers should explore whether economies of scale could be used to make a market for SMB cyber security solutions more attractive and financially viable for both buyers and sellers. There are likely multiple mechanisms possible to address the issue, such as consortia and combined purchasing agreements. Intel recommends policymakers work with the Small Business Administration and other SMB advocates to understand the market drivers and any existing programs.

CONCLUSION

Thank you again for the opportunity to address the Committee. I will be happy to answer any questions.