Testimony before the Committee on Small Business: House of Representatives

Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option
H.R.3170 - Small Business Development Center Cyber Training Act of 2017

Statement of:
Daimon Geopfert, Principal and National Leader of Security, Privacy, and Risk at RSM US LLP

Background

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for the opportunity to discuss the cyber security challenges that have become a constant, material threat within the small business community. My name is Daimon Geopfert, and I was asked to speak today regarding how legislation such as H.R 3170, and private sector solutions such as cyber insurance products, can help small organizations manage cyber risk. I spent almost 14 years within the Department of Defense (DoD) including 12 years as active duty Air Force, officer and enlisted, and two years as a defense contractor building Security Operations Centers (SOCs) for various government agencies. While on active duty, I was a secure communications specialist, a Computer Crimes Investigator (CCI) with the Air Force Office of Special Investigations (AFOSI), and a cyber specialist within the Air Intelligence Agency. Since leaving the DoD, I have spent the last ten years as a security consultant, initially with a “Big 4” firm and now as a principal with RSM US LLP (“RSM”), where we specialize in cyber security consulting within small and middle-market businesses. My specializations include ethical hacking, security monitoring, digital forensics, incident response, and malware analysis.

During my career, I have participated in hundreds of security assessments and cyber intrusion investigations for small businesses. Because of my role, I am often in a position to witness every stage of an attack within these organizations, including the devastating economic and emotional impacts that often linger after the technical aspects of the issue are resolved. On more than one occasion, I have had to sit with a client, who is often uninsured, explain to them the extent of a breach, and listen to their anguish as the realization sets in that their business might not survive the costs related to an incident. In my profession, there are few things more painful than listening to a client debate how they are going to inform their employees that they will soon be unemployed, or to listen to

a family-owned business lament that their legacy, which might span generations, will simply cease to exist.

Purpose

I am here today in the hope that my experiences can play some small part in addressing this issue, which appears destined to be a continuous, ever increasing threat to the U.S. economy. My role has allowed me to observe the many weaknesses that, if corrected, would have an exceedingly positive impact on a small business' ability to prevent, or at least survive, future incidents. These organizations want to do the right thing, even if out of simple self-preservation, but they often lack the means to acquire the necessary resources to actually understand and execute what must be done. What is needed is a venue through which small businesses can find simple, direct guidance on how to protect their environments and mitigate risk, and that also provides access to resources with the necessary expertise to chaperon them through implementation of that guidance.

Legislation such as H.R 5064 and H.R. 3002 were both early attempts by this body to modify the Small Business Act to allow the Small Business Development Centers (SBDCs) to begin serving such a role. The current H.R. 3170 legislation addresses part of this requirement by essentially creating "cyber mentors" within the SBDCs. These personnel could quickly become the front-line advisors that are desperately needed to guide small businesses through the deployment of technical security solutions as well as administrative risk management techniques such as acquiring cyber insurance. It should be noted that this is very close to the how the Cyber Essentials program works within the United Kingdom. This approach has proven to be quite successful at mentoring small businesses through a basic cyber hygiene program including acquisition of cyber insurance.[i] Not providing access to resources of this nature is no longer a viable option, as it is essentially conceding that approximately half of the U.S. economy should be left to defend themselves against highly skilled attackers in search of money, intellectual property, and nation-state political advantage.

Current State

While serving within the Department of Defense, I had unfortunate opportunities to witness how aggressive, persistent, unpredictable, and innovative cyber attackers can be. After leaving the DoD, within two years I saw these same perpetrators appearing within my private sector clients. Understand that these attackers were skilled enough to give the DoD pause, much less the IT teams within small business and the middle-market. In reality, the situation is even worse than that which I faced within Defense

networks at the time I transitioned. Historically attackers were limited by the extent of their own personal expertise. Now, hacking experts consolidate their skills into pre-packaged “kits” available to anyone who can find their way into the underground market and scrape together a few thousand dollars. Each of these packages comes with full tech support, simplified graphic interfaces, and detailed, easy to follow guides meant to allow a relative newcomer to become “pseudo-elite” virtually overnight. This has significantly lowered the knowledge threshold necessary for someone to act like a world-class hacker, and has increased the number of attackers going after U.S. business by order of magnitude. We are basically facing an army of highly effective “cyber soldiers” who have no actual understanding of what they are doing or how their tools work, but they do know if they point it at an company and click the correct buttons, they almost magically make money.

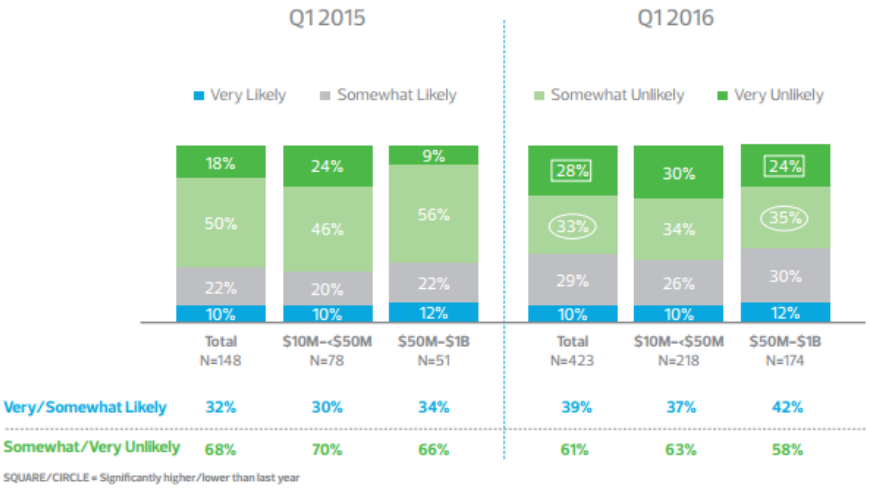
The reality for small and middle-market companies is that the Internet has reached a fundamental, “utility” type status, as it is now a required piece of infrastructure for almost any organization to be successful in our modern economy. However, this powerful asset that is essentially required for branding, sales, management, and growth, is also incredibly hostile and toxic to systems, networks, and users. U.S. small businesses face a situation in which they are required to use an environment that is highly likely to damage, or even destroy, the finances, assets, and reputations of their corporation or those of their customers. Arguably, for the first time in our economic history, a major portion of a business’ effort and expense is consumed by something that has very little to do with their core business but is required in order to exist. Small business are being forced to be become IT and cyber experts in addition to trying to establish, deliver, and expand their core services. This model can work for large organizations, but it does not scale to small businesses.

While a wide array of security software, hardware, and frameworks are available, small organizations typically lack the resources to properly acquire and deploy them. Many tools and frameworks are built for large organizations with significant funding and on-hand IT resources. Many of these do not scale down well to fit small and middle-market businesses, and the “lightweight” and open source tools that might be cost-effective for small organizations often require extensive IT and security knowledge to properly deploy.

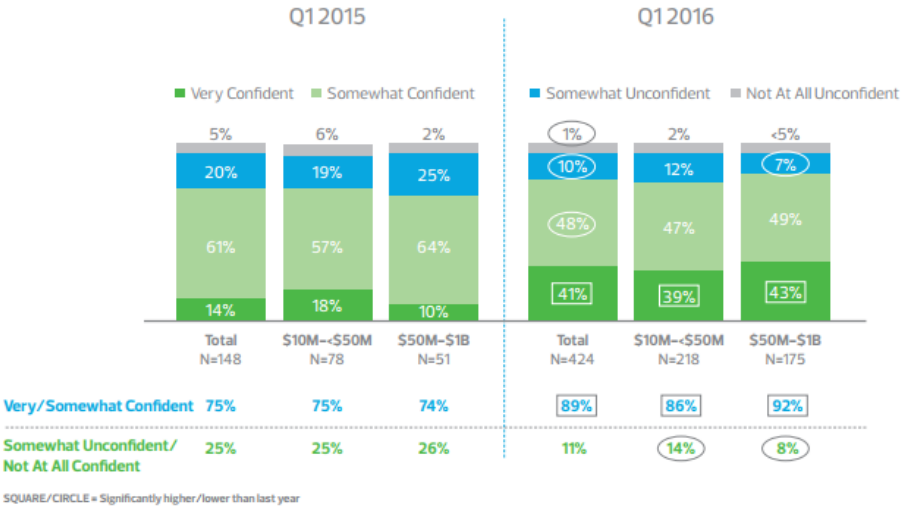
Cyber insurance has gradually assumed an important role in this process, but the current state of security governance within small organizations limits the benefits and uptake of this risk mitigation method. Many organizations simply do not understand the likelihood that they will be breached, and often severely underestimate the damages if such an incident were to occur. Much of this is an issue with education as extensive coverage of “mega breaches” such as Target has led many small and middle-market organizations to

rationalize to themselves that they are too small for attackers to notice. RSM participated in two keystone studies this past year that highlight how drastic the gulf is between perception and reality in regards to cyber threats to small businesses. In the first study, RSM surveyed more than 700 executives within American small and middle-market companies to assess a variety of economic and business factors influencing their planning for the coming year.[ii] Included in that survey was a series of questions regarding cyber security. More than 60 percent of these organizations felt that it was unlikely that an attacker would attempt to attack their business systems, and approximately 90 percent of the respondents felt that their currently deployed controls would be successful in preventing such an attack. This was almost a 15 percent increase over the prior year, which shows that small organizations do not perceive themselves as being targets and do perceive themselves as being relatively skilled at cyber defense.

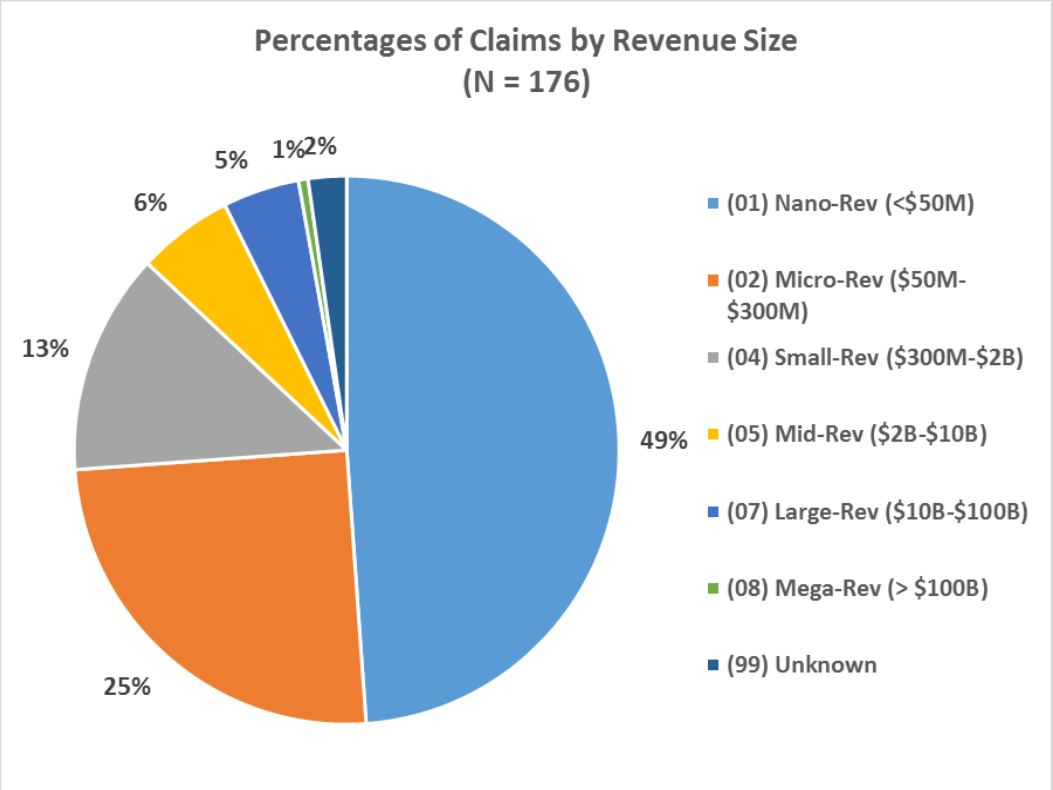
LIKELIHOOD UNAUTHORIZED USERS WILL ATTEMPT TO ACCESS SYSTEMS



CONFIDENCE IN MEASURES TO SAFEGUARD DATA



Regrettably, the reality of the situation cannot be further from this illusion of confidence. In the same time period in which RSM was surveying small business executives, we teamed with the analysis group NetDiligence to perform extensive data mining within a population of cyber insurance claims.[iii] That review showed that approximately 75 percent of cyber insurance claims submitted over the period of the study were for organizations under $300 million in revenue. Approximately 50 percent of the claims were for organizations $50 million in revenue, and the damages reported for these small businesses were similar to the damages occurring in organizations tens, or even hundreds of times larger.



Total Costs (including SIR)					
	Cases	Min	Median	Mean	Max
(01) Nano-Rev (<$50M)	85	290	49,000	215,297	7,130,000
(02) Micro-Rev ($50M-$300M)	44	1,000	88,154	487,411	6,570,000
(04) Small-Rev ($300M-$2B)	23	4,178	118,671	599,907	5,650,000
(05) Mid-Rev ($2B-$10B)	9	2,662	91,457	173,851	678,000
(07) Large-Rev ($10B-$100B)	8	1,603,800	3,326,313	5,965,571	15,000,000
(08) Mega-Rev (> $100B)	1	11,491,000	11,491,000	11,491,000	11,491,000
(99) Unknown	2	7,338	9,482	9,482	11,625
	172				

These percentages had actually increased over the analysis performed the prior year, which shows that attacks against small business are not an anomaly; they are the norm. This is the key demographic targeted by hackers, and the aggressiveness of their attacks is increasing. Yet at the same time, confidence levels of small organizations were

approaching an all-time high. This leads to a type of cognitive dissonance in which small organizations acknowledge that cyber-attacks have become ubiquitous and highly potent, but, at the same time, they convince themselves that they will not be targeted, and if they are, they feel that their defenses would fend off any malicious actions. This extreme inability to accurately quantify their risk leads many small organizations to determine that allocating precious resources toward security solutions and cyber insurance is unnecessary. This leaves many organizations operating without any type of fiscal safety net meaning they would carry the full brunt of any expenses, bank account thefts, ransoms, civil damages, and fines stemming from an incident. As multiple studies have shown, even a single incident will put approximately 60 percent of small organizations out of business within six months. [iv]

However, even when a small business has acquired insurance, in the event of an incident the generally immature nature of their security controls often greatly compounds costs for both the victim and the insurance carriers. They simply are not ready for the process of going through an incident. They assume that they will know very quickly when they have been breached, but independent research by multiple security firms over the last five years indicates that an attacker will likely be inside an organization for 200-300 days before they are discovered. This means many organizations will build their response plans assuming they can prevent damage, but, in reality, they need to be skilled at performing post-facto accounting of what hackers did while they were within an environment. Lack of proper logging means that an organization might know that an attacker was in their environment but be unable to reconstruct the story of what that attacker touched, where they went, and what they took. This puts many small organizations in the position where they must assume the worst, and perform mass notifications to any individuals that theoretically might have been impacted, where larger, more mature organizations often have the evidence available to properly allocate the hacker's activities and, therefore, greatly reduce the size of the reported breach. Because small businesses often lack formal incident response planning, when they do become aware of an issue, they often attempt to address it themselves using a variety of unplanned activities that usually damages or destroys what little evidence might have existed. These are the major contributing factors why data breaches are inordinately harmful to small organizations, as they often must pay damages based on assumed worst-case events. This also leads to cyber insurance carriers often having difficulty pricing the risk that small organizations represent. It is difficult to justify premiums and deductibles that are tolerable for organizations with small revenue, when those same companies can easily generate damages equal to organizations an order of magnitude larger.

Requests

To make tangible progress on this issue, small businesses need ready access to resources and information that is currently unavailable to them because they often cannot afford dedicated personnel with the necessary knowledge and skill-sets. Legislation such as H.R. 3170 can start the process to create a cadre of trained personnel within SBDCs who can directly mentor these small businesses that are so critical to the sustainment our economic future. These personnel can essentially become “virtual Chief Information Security Officers” across entire groups of small businesses. Currently, small businesses attempt to acquire security guidance through a variety of security vendors and consultants, but many of these groups have trouble “scaling down” their guidance to be appropriate to environments that do not have the scale and resources of a Fortune 500 organization. Cyber counselors within the SBDCs would be relatively unique within the security community in that they would be solely focused on planning and deploying cyber strategy that is efficient and pragmatic for small businesses. Because their role allows them to interact with a large number of companies, the SBDC counselors become a de facto knowledge sharing center carrying best practices from one business to another. They would see in real-time what technologies and processes are effective within a small business, and which ones are not.

While educating and deploying a “first line” of security advisors within the SBDCs is a critical first step, these facilities hold the promise of a myriad of other benefits that could be made available in the future. Again, to make material progress on this issue we need to move toward clear, concise, pragmatic solutions. While it might seem like an abnormal suggestion, a primary goal of the SBDCs should be to emulate their peers in the hacking community. We are currently lacking the process on the defensive side that exists on the aggressor side, in which relatively non-technical individuals can become highly effective in a short period of time. As mentioned previously, the underground markets have become exceptionally efficient at quickly churning through masses of unskilled individuals with limited technical knowledge and producing a large number of, while not elite, at least functional cyber attackers.

Similar to the methods of our adversaries, small and middle markets need a dedicated hub where they can find useful, cost-effective tools and simple, pragmatic guidance on how to deploy security solutions that, while not elite, are at least complete and effective at a basic level. Existing frameworks from organizations such as the National Institute of Science and Technology (NIST) are high-level and extensive which might be appropriate for large organizations, but they are of little to no value to small organizations that require

low-level, step-by-step guidance on how to achieve some moderate baseline for security. In conversations with executives within the small and middle market regarding my testimony today, this is far and away the most frequent request. What they are looking for is what the security community would describe as “reference environments”, which are top-to-bottom, detailed layouts of basic networks with common security controls. As an example, reference environments can be created for networks that are exclusively on-premises, those they rely heavily on cloud solutions, or almost any other model that is common within the small business community. In addition, versions can be quickly adapted to reflect the needs of businesses within specific industries such as retail, manufacturing, and healthcare. These reference environments often detail what security solutions must be deployed, how they must be configured, how data should flow through the network to maximize protection, how users, customers, and third parties should be granted access, and any number of common security requirements. While it sounds relatively simple, these types of assets are not common in the small business community, which often leads to organization cobbling together their security architecture based on their individual interpretations of high-level frameworks that are often more academic in nature than they are prescriptive. The SBDCs could play a critical role in the process of creating and disseminating such models.

The benefits of deploying such common models extends well beyond the immediately visible increase in technical security. As an example, the second most common request during my conversations with executives was for actionable cyber threat intelligence that could be easily consumed and put to use by a small business. This would include notifications of known bad IP addresses and URLs, signatures for new malware and exploits, and Indicators of Compromise (IOCs) that would alert an organization to the presence in their network of known hacking groups. Currently it is extremely difficult to meet this need because information must be shared in high-level, agnostic formats that can be used by a wide variety of organizations. If common reference environments are made available to small businesses, many of these entities would be highly interested in using those frameworks if they knew that it would allow them to access and use real-time threat intelligence in an almost “plug and play” fashion. The development of such reference environments would require extensive cooperation between the government and private sector entities, and a designated coordination and distribution point of threat intelligence, both of which are obvious roles that could be played by the SBDCs. It should be noted that support of this type was included in the prior H.R 5064 legislation that passed in this Committee last year, but has still not been acted upon in the Senate.

This could eventually lead to the SBDCs acting as the primary coordinator between the small business community, government, and private sector security vendors in creating a

set of approved solutions and services that are “right sized” for small businesses. Potential future legislation could even allow the SBDCs to negotiate with the security industry to purchase solutions “in bulk” for use by pools of small businesses. Currently, each small business individually negotiates with a wide variety of security vendors and consultants, which creates wildly inconsistent pricing and results. While this is always an option for organizations that feel that they are mature, sophisticated buyers of these services, many other organizations would gladly accept assistance from a community of similar consumers. With an entity such as the SBDC doing "pooled" pricing to drive down costs and standardizing the level of services, the small business community would have access to much more cost-effective solutions that would also produce more consistent results. These benefits can be further expanded if the SBDCs coordinate with the private sector security industry so that versions of their cyber solutions can be certified as being compliant with the reference environments. This would allow small businesses to acquire services knowing that they are an appropriate fit for their organizations, while also allowing security vendors to cater to a large pool of potentially new clients. It would be a classic “win/win” situation for all parties involved.

At this point the foundations would be laid for a base level security accreditation program for small business in which they can demonstrate that they have deployed basic cyber security controls and processes. This would be very similar to the UK Cyber Essentials program. The SBDCs, which at that point would be acting as a centralized body in publishing the reference environments and coordinating with private sector security vendors, would be a natural fit to oversee this program. An outcome from this approach would be that the SBDCs could then coordinate between newly accredited small businesses and insurance carriers to facilitate the acquisition of cyber insurance for these organizations. These suggestions create a process that would then naturally flow from a set of standardized security templates, through approved, cost-effective technologies that meet those templates, to an accreditation program that validates that the solutions were deployed correctly, and finalizes with the purchase of cyber insurance to offset the residual risk. This process, in its entirety, represents the most requested types of support by small business executives encapsulated in a clear, concise, and pragmatic approach, and it would materially improve the current security status of approximately 50 percent of the U.S. economy. [v]

While the development of such a standardized process will deliver the most significant results over the long-term, it must be recognized that there are several other immediate, tactical needs that the SBDCs could also address in the near future. Of specific importance is the facilitation of security training within small businesses. Prior legislation, such as H.R 5064, was aimed at starting this process by making security awareness

training available to the employees of small businesses to reduce the likelihood that they would fall for common types of social engineering. While this type of training is extremely beneficial, the concept of performing training through the SBDCs could be greatly expanded. As mentioned previously, the core issue preventing small and middle market companies from becoming properly secured is the inability to acquire access to trained security personnel. While government programs can provide significant assistance to these companies, the beneficial impact will always be limited until small businesses can develop or hire their own security resources. However, the reality of today's jobs market means that these trained individuals are rare, expensive, and difficult to retain for any extended period of time. Recent studies by the U.S Department of Commerce and NIST show that of the entire U.S. workforce considered to be trained cyber security personnel, enough job openings exist that half of that workforce could quit their jobs today and have new employment tomorrow. In further detail, the study showed that the number of positions that request the most respected security certifications outnumber the total population of personnel that have those certifications by as much as 2 to 1 in some cases.[vi] This critical skills gap prevents small and middle market companies from acquiring top security talent, which then drives the need for them to develop their own. H.R. 3170 is written to provide cyber security training to counselors within the SBDCs, but similar future legislation could follow the same model with the goal of providing training directly to the IT personnel within small businesses. This could be as simple as basic "how to" guides for common tasks such as deploying patch management and access control systems, or could be as robust as coordinating with the private sector to offer reduced prices or subsidized versions of critical training programs such as those for incident response and secure network architectures.

My final point is a request meant to address an issue that is easily the most tortuous and aggravating for small business. While this might be through the SBDCs or through some other mechanism, it would be highly useful to have a designated, prescribed method through which small businesses can coordinate with a law enforcement entity that is responsive and functional when it comes to cyber breach matters. Currently, when a small business is compromised, they are often given two potential choices. They can contact their local police departments which are usually willing to help but lacking in the skills to do so, or they can contact the Federal Bureau of Investigations (FBI) or U.S. Secret Service (USSS) who have the ability to help but typically do not have the availability to do so unless the breach has extremely substantial damages. Imagine the frustration felt by a small business owner who has suffered what might be an "end of going concern" level incident, then realizing that they are essentially on their own because the law enforcement entities that will help lack the skill-sets to do so, and the law enforcement entities that have the skill-sets are not willing to do so. This situation has

created the mindset within the small business community that, when it comes to cyber matters, they have essentially been abandoned in the “wild west” where the rule of law does not apply. It would be extremely beneficial for a process to be put in place to give small businesses rapid access to a law enforcement entity that can, and will, support their response. This is not to suggest that the goal of this support is to end every incident with an arrest and prosecution. With the simple reality that many attackers are operating out of geographies where the U.S. has no jurisdiction, it is not reasonable to assume that arrests would be common. The goal of this law enforcement involvement is to facilitate rapid and complete investigations of issues so that damages can be reduced as much as possible. As an example, it is common during an incident investigation to discover that attackers were coming from another system within the U.S.. If a small business does not have the proper logging and other sources of evidence necessary to reconstruct the entirety of a breach, and therefore know the true extent of data loss, there is often the chance that the necessary evidence is located on the system from which the attacker entered the environment. The ability to get a law enforcement entity involved quickly can mean search warrants might be used to gather logs, files, or other artifacts from internet service providers (ISPs), systems in other companies, or systems owned by individual citizens. We often try to perform these actions today, but the process is so time consuming that viable evidence is often lost before we can acquire it.

Legislation that addresses the points I have described above would greatly improve the security and longevity of U.S. small and middle market businesses. These entities are the core of U.S. growth and job creation, but they are under daily siege from cyber adversaries. If our political institutions cannot find a way to assist these organizations, the U.S. economy, and arguably our role as the premier member of the global economy, will be under dire threat for the foreseeable future.

Conclusion

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other members of the Committee might have.

The views expressed herein are those of Mr. Geopfert, and are not necessarily those of RSM US LLP.

Daimon E. Geopfert

National Leader and Principal, Security, Privacy, and Risk Consulting
Risk Advisory Services
RSM US LLP
Chicago, Illinois
daimon.geopfert@rsmus.com
+1 312 634 4523

Summary of experience

Daimon Geopfert specializes in penetration testing, vulnerability and risk management, security monitoring, incident response, digital forensics and investigations, and compliance frameworks within heavily regulated industries. Daimon has over 20 years of experience in a wide array of information security disciplines. He serves as the firm's national leader for the security, privacy, and risk practice, responsible for the development of the firm's overall strategy related to security and privacy services and applicable methodologies, tool kits and engagement documentation.

Daimon is a regular presenter for organizations such as Information Systems Audit and Control Association (ISACA), InfraGard, the Certified Fraud Examiners and SC Magazine's World Congress. He has been quoted in a variety of publications, including The Wall Street Journal, Fortune Magazine, The Washington Post and the Kansas City Business Journal.

Representative experience

- Information systems security assessment
  Daimon has served as the manager and lead technician for security assessments performed on some of the largest corporations and government entities in the world. He has designed and implemented testing frameworks and methodologies used to properly capture and communicate the technical, operational and regulatory impact of identified security weaknesses.

  Daimon's experience in this area includes analyses and reviews of the following:

  - Security testing across the enterprise: network, host, application and database
  - Wireless, Voice over Internet protocol (VoIP), cellular, modem/telco assessment
  - Security operations structure and effectiveness
  - Social engineering testing, including phishing/pharming, phone and physical
  - Corporate security policies and procedures
  - Application secure architecture and coding analysis

- Incident response, forensics and security monitoring
  Daimon acts as the lead developer for RSM's forensic and monitoring service offerings, and has designed and deployed incident response and security monitoring programs within several highly regulated clients. These frameworks are based on customized versions of National Institute of Standards and Technology (NIST) SP800-81, ISO 18044:2004 and the SANS IR 6 Step. Daimon previously served as a special agent with the Air Force Office of Special Investigations as a researcher with the CIA's Directorate of Science and Technology, and deployed and ran Security Operations Centers for the Department of Defense (DoD).

- Security program management
  Daimon has managed and performed a myriad of security program engagements across a variety of industries. The purpose of these projects was to assist organizations in deploying efficient, manageable and cost-effective solutions and processes that would address the wide ranging business and regulatory aspects of IT security. Daimon has deep experience in Payment Card Industry (PCI), HIPAA/Health Information Technology for Economic and Clinical Health (HITECH), FFIEC/Federal Deposit Insurance Corporation (FDIC), Federal Information Security Management Act (FISMA), NIST SP800 series, ISO 2700X, National Information Assurance Certification and Accreditation Process (NIACAP)/DoD Information Assurance Certification and Accreditation Process (DIACAP), American Electric Reliability Corporation(NERC)/Critical Infrastructure Protection (CIP), EU Data Privacy Directive, and various state security and privacy laws.

Professional affiliations

- Information Systems Audit and Control Association (ISACA)
- International Information Systems Security Certification Consortium (ISC)^2
- FBI InfraGard, Michigan Chapter—Member, Presenter, Speaker Committee
- The SANS Institute—Global Information Assurance Certification (GIAC)
- The Ethical Hacker Network

Professional certifications

- Certified Information Systems Security Professional (CISSP)—(ISC)^2
- Certified Information Security Manager (CISM)—ISACA
- Certified Information Systems Auditor (CISA)—ISACA
- GIAC Certified Incident Handler (GCIH)—The SANS Institute
- GIAC Certified Reverse Engineer of Malware (GREM)—The SANS Institute
- Certified Ethical Hacker (CEH)—EC-Council

Education

- Master of Science, computer science, University of Michigan
- Bachelor of Science, computer science, United States Air Force Academy
- Numerous technical and industry courses and seminars

[i] IASME Consortium, “Automatic Insurance Cover ”https://www.iasme.co.uk/cyberessentials/automatic-insurance-cover/

[ii] RSM, “US Middle Market Leadership Council Survey Report” (http://rsmus.com/pdf_download/rsm_middle_market_leadership_council_survey_may_2016.pdf)

[iii] NetDiligence, AllClear ID, RSM “2016 Cyber Claims Study” (https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf)

[iv] U.S. Securities and Exchange Commission, “The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses” - Commissioner Luis A. Aguilar, Oct. 19, 2015 (https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html#)

[v] Small Business Administration, “Small Business Trends” (https://www.sba.gov/managing-business/running-business/energy-efficiency/sustainable-business-practices/small-business-trends)

[vi] National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology in the U.S. Department of Commerce, “Cybersecurity Supply/Demand Heat Map” (http://cyberseek.org/heatmap.html)