Testimony Submitted by

Rob Arnold, CEO & Founder of

Threat Sketch, LLC

https://threatsketch.com

before the

House Small Business Committee November 15, 2017

Data Sharing

My company, Threat Sketch, makes extensive use of shared information to educate small businesses and guide their investments in cybersecurity. We are a small business ourselves, and I have written extensively on the subject of managing cyber risk using information based tools and methods[1]. Thus, I truly understand the needs and challenges around sharing cybersecurity information, of which there are two broad types.

1. *Incident reporting* refers to an after the fact report of companies that were attacked. It includes victim demographics, methods of attack, and losses incurred.
2. *Cyber Intelligence* generally refers to leading indicators of attack, and examples include newly discovered software vulnerabilities, suspicious activity, signatures of malicious software, and information about adversaries such as new capabilities.

[1] Arnold, Rob (2017). *Cybersecurity: A Business Solution*. ISBN 978-0692944158.

Fragmentation

The most fundamental problem in accessing this data right now is fragmentation. The DHS, FBI, NIST, and the NSA, are just a few of the agencies collecting cyber incident and intelligence information. Each has multiple repositories and programs. Some are well advertised, while some are part of workgroups and not widely available. Others are hidden by classification. Simply having a list of all the data sharing initiatives available would help tremendously.

Such a list might start with the various Information Sharing and Analysis Centers (ISAC's) and Information Sharing and Analysis Organization Standards Organizations (ISAO's), and expand to include to programs like DHS's Automated Indicator Sharing (AIS) program. The inventory would include what information sources they consume, how they make the data available, and the membership criteria for each. The intermediate organizations like ISAC's and ISAO's are, in many cases, doing a great job of making otherwise inaccessible data available to small businesses[2].

Small businesses are extremely resourceful. Having quality incident reporting and cyber intelligence flowing to the small business community lets us build solutions for ourselves.[3] Our biggest challenge, in that regard, is collecting and aggregating data from a wide array of sources. In truth, even the largest multi-national companies cannot collect data on the breadth and scale that US government agencies can provide. Access to quality data for companies of all sizes helps level the playing field between large and small businesses and will spur economic development alongside novel solutions.[4]

[2] See Appendix: How the IT-ISAC makes AIS affordable
[3] See Appendix: Email Interview: Douglas M. DePeppe - Cyber Resilience Institute
[4] See Appendix: Economic Trends And How Shared Information Helps

Overuse of Classification

Another problem with sharing information is the overuse of classification. There are a myriad of rules governing the declassification of information, but declaring valuable information a secret is almost effortless. It takes no more than two words, uttered in a grave tone, to play keep away with vital information. "*That's classified*." And just like that, our cyber equivalents of neighborhood crime statistics and sex offender registries are taken away in the name of national security. While secrets have their place, we have a right to know what is going on around us, and every data point that gets classified degrades our ability to make good decisions[4,5].

The other problem with classifying information is that it creates another digital divide between the have's and the have not's. Small companies are generally much better at raw innovation. When we cannot get access to the raw material for building novel solutions, our security posture will not improve and we lose economic opportunities to create jobs around our innovations.

As you contemplate the role of classification, please keep this in mind: When this country was founded, we were colonists living under the boot of a government that exerted control by keeping secrets and forcing access to information it deemed might be incriminating. Our adversaries would like nothing more than to goad our government into keeping secrets, then unleash those secrets to draw the ire of the citizens and undermine trust. Remaining transparent is the only solution that works in the long run. It is better that we let our enemies know we see them coming and face them head on, than to have us bickering with one another while they steal all our trade secrets[5].

[5] See Appendix: How Classification Impacted the Wannacry Outbreak and Response

Pressure to Keep Up Poses Major New Threat

There is a more pressing issue to which I need to draw your attention. It is a byproduct of two distinct disadvantages that small businesses face:

1. As big companies armor up, attackers turn to less protected small businesses.
2. Small businesses cannot afford to compete with big companies for the cybersecurity talent and solutions they need to protect themselves.[6]

These are circular issues with one begetting the other. In their wake, the demand for affordable solutions will rise dramatically, creating yet another threat. Small businesses desperate to meet the cybersecurity demands of larger clients, government regulations, insurance carriers, and lending institutions are going to become victims once again. Adversaries will use this opportunity to sell cheap software and services that are subsidized by selling data and secrets out the back door and give them a toehold in the supply chain of larger organizations.

The driver here is that cybersecurity is also economic warfare and a geopolitical game of chess that knows no borders. These higher-level battles manifest as foreign and domestic espionage, extortion, and economic disruption. They encompass aspects of both organized crime and the Cold War. A central issue that impacts small businesses is the ability to vet vendors who may have ties to either the criminal underground or nation-state adversaries.

Deputizing Small Business Cyber Solution Providers

I believe we can get ahead of this problem with your help. Fixing the problem with American-made products and services will not only protect the sector, but also stimulate job growth and economic development. I suggest that the SBDC's work with local, state,

[6] The federal government is also snapping up scarce talent. For example, students can receive scholarships worth up to $60,000 for NSA accredited degree programs, but then they are obligated to work for the government. Small businesses cannot compete with that kind of recruitment.

and federal law enforcement to certify local vendors as All-American solution providers, then connect those vendors with other SBDC's within their state and across the nation.

Participants would be bound to:

- defend small businesses under a Hippocratic-like oath,
- affirm allegiance to US interests,
- produce software/services domestically (no offshoring data or talent), and
- report cyber intelligence using uniform methods.

Participants would be subject to steep legal penalties for using offshore solutions, perhaps submitting to spot-check investigations to ensure compliance. However, so long as they rely on American solutions, they (and perhaps their clients) would be protected by good-Samaritan laws much like our first responders. These deputized small businesses would also form a sort of national guard embedded directly in our business communities.

Improving the Collection and Dissemination of Information

In addition to tapping our SBDCs, I believe the government has two resources that can help with collection and dissemination of cybersecurity information. Our Bureau of Labor Statistics (BLS) is very good at aggregating, summarizing, and making data available in easy to digest forms. Meanwhile, the IRS is one agency to which every small business owner is happy to report losses.

Obviously there is potential for abuse in reporting losses that did not occur. To offset this, any loss report would trigger (or could trigger in the case of a lottery system) an investigation by law enforcement to validate claims. The investigation would allow for the gathering of valuable incident details and cyber intelligence information.

The DHS was established to bring together intelligence and data from multiple agencies. Therefore it makes sense to have data bubble up to them for aggregation and, when absolutely necessary, apply *judicious and time-limited* classification. Gathering points for information would include the IRS, as mentioned above, but also local/state/federal law enforcement, with SBDC advisors connecting small businesses to them as appropriate. In fact, it may be best to classify all data initially at the gathering points and charge the DHS with declassifying *everything*, except that which is truly vital to national security or conflicts with privacy. Doing so alleviates the SBDC advisors, law enforcement, and any deputized businesses from making such decisions.

While DHS has the ability to aggregate and (de)classify data, the Bureau of Labor Statistics (BLS) has the talent, infrastructure, and existing relationships to repackage and deliver it back to the community. Undoubtedly some will insist the data need not be made public. But security by obscurity only builds false hopes.[7] In fact, I would argue that the value added from the statistical expertise to *correctly* interpret raw data would far outweigh the idea of keeping poorly interpreted data secure.

An example of poorly interpreted data is the oft-quoted statistic that sixty percent of small businesses fail within six months of a cyber attack. It is so tantalizing,\ that even we used it at Threat Sketch early on in our marketing materials. However, we later learned this to be unverified information and have distanced ourselves from it because our clients trust us to deliver accurate data.[8]

SBDC Advisor Training

Small businesses need local solutions that can tap into a national network of trusted solution providers. The SBDCs have proven effective in helping small businesses navigate a myriad of state, federal, and local resources, and with training, I believe they can rise to this challenge as well.

[7] See Appendix: How Classification Impacted the Wannacry Outbreak and Response
[8] https://www.bankinfosecurity.com/blogs/60-hacked-small-businesses-fail-how-reliable-that-stat-p-2464

With regard to training, the NSA has been busy establishing a network of colleges and universities that are Centers of Academic Excellence (CAE) in Cybersecurity. And NIST, through its National Initiative for Cybersecurity Education (NICE), is helping standardize the language in our industry, which is much needed. I believe that the NSA-CAE community colleges and universities are well positioned to cross-train and up-train existing SBDC advisors on the ***business aspects*** of cybersecurity. Advisors need not become technical experts, but rather learn the standardized language developed by NICE and delivered through NSA-CAEs. Doing so will let them help small businesses locate and connect with appropriate resources.

Appendix

How the IT-ISAC makes AIS affordable

The DHS has an information sharing program called Automated Indicator Sharing (AIS) that gathers and distributes cyber intelligence using STIX and TAXII protocols. When I first encountered this program through Threat Sketch, the only commercially supported software systems had six-figure price tags. Although free, open-source versions exist, they require constant patching and maintenance as well as a secure facility to house them. These hidden implementation costs put “free” information well out of the price range of small businesses.

We were referred by AIS to the IT-ISAC, which already had infrastructure in place to receive AIS information via STIX/TAXII and was able to fractionalize the cost among its paid members. The IT-ISAC has since played a vital role in both supplying data and allowing us to share our own knowledge back to the community.

Email Interview: Douglas M. DePeppe - Cyber Resilience Institute

> *Cyber Market Development Project, as well as Sports-ISAO Project Office. Our nonprofit, Cyber Resilience Institute, is the NIPP Challenge awardee (and our project will transition to commercial use under ‘c-Market’ branding and naming). Our model has a CTI and Information Sharing core, based in a community and adopting a PPP sharing and capacity building model.*
>
> *That as a quick background, we enter communities through students and a workforce program: c-Watch. And, what we’re promoting is the linking together of a network of cyber hunters and analysts – that is, graduates of the workforce program – into the Cyber Threat Intelligence Research Network. What CTIRN represents is a national capability of students – a bit like a CyberCorps or a*

cyber-ROTC equivalent – engaged in populating a commercial Order of Battle (i.e., adversary profiling), that would be available for the private sector and all levels of government, and without incurring IC classification constraints.

How Classification Impacted the Wannacry Outbreak and Response

I participated in the national response to the Wannacry outbreak lead by the National Cybersecurity and Communications Integration Center (NCICC; pronounced "N-KICK"). During one of the daily NCICC calls, a large company claimed to have something they wanted to share, but did not want to make it public. A DHS representative came on the line and declared the briefing TLP-Yellow from that point forward. He then invited all companies on the line to share what they knew and there was nothing but awkward silence. Even under a veil of secrecy, the big company was unwilling to share what they knew. I wonder to this day what it was and if it could have saved even one victim.

And let us not forget that the reason the Wannacry outbreak was able to travel so quickly. It did so by leveraging an exploit discovered by the NSA and kept secret until exposed in a WikiLeaks data dump. I understand why the flaw was kept secret, but that decision was not without consequences. The entire attack may never had occurred had the flaw been disclosed to the private sector when it was first discovered. Not only did that decision lay the groundwork for the ransomware attack, but it created a rift between the government and the private sector. I know of at least one large-scale flaw that was not reported to the government for the reason that cybersecurity researchers have lost faith in our government. It will take a long time and many taxpayer dollars to recover from the tarnished image that results from keeping secrets.

Economic Trends And How Shared Information Helps

To describe how shared cyber incident and intelligence information helps small businesses, I need to provide context. At a company level, cybersecurity is a business

problem of risk management. At a national level, cybersecurity is economic warfare. At a global scale it is a geopolitical game of chess that ignores physical borders.

At the business level, three trends drive cyber risk in small businesses. They are:

1. An increase in incentives for hackers to make money by exploiting stolen data.
2. A dramatic rise in the liability that comes with handling sensitive data.
3. The use of automation to attack small businesses on an industrial scale.[9]

Let's use a familiar example to illustrate how these three forces have changed the risk landscape. Consider an employee's W-2 form. Ten years ago it was hardly worth the paper it was printed on because there was no mass market for selling personal information. Today, each W-2 is worth $20 or more on underground, black markets. The incentive has gone from nearly zero to $20 dollars per victim.

While the hacker gets $20 for each W-2, the ***liability*** to the employer and the employee is substantially higher. In the extreme, lawsuits and drained bank accounts can cost the business and the employee hundreds of thousands of dollars. And more subtle losses come in the form of lost morale and the hassle of dealing with damaged credit, which add to the losses.

While there is an incentive to steal W-2s en masse from large companies, the big companies are becoming harder to attack. As a result, hackers are using automation to go after unprotected, unprepared small businesses by the thousands. Due to the volume of attacks, they only need to compromise a small fraction of them to make a profit. It is a nefarious business model that works.

In the context of trend number one, sharing cyber intelligence about black markets and espionage warns small businesses about emerging incentives for stealing data. To

[9] Arnold, Rob (2017). *Cybersecurity: A Business Solution*. ISBN 978-0692944158.

address the second trend, which is victim liability, incident reporting is used to understand trends in the risk landscape and to determine how different attacks relate to losses. Finally, combatting automated attacks means using both types of data to detect large scale operations and respond quickly to undermine the nefarious business model.