Cybersecurity Development Coalition: Proposal for Action

Cybersecurity threats to all organizations continue to grow – but the development of defenses across small organizations has not. While smaller organizations may not have the same security needs as larger business enterprises, many elements can be shared across sectors. A small business might house some critical personal information about clients, a non-profit might be large and distributed internationally. The Cybersecurity Development Coalition (CDC) is a model for improving information and network security in small and mid-sized organizations through mentorship and peer networks.

The Problem

The Big Picture

The risks to organizations associated with operating online have increased dramatically in recent years.[1] The necessity for utilizing a variety of connected tools in the workplace has created an increasing number of opportunities for a continually growing field of attackers. The variety of threats has been documented by the increased focus of major media outlets and policymakers at all levels of government. Large businesses and organizations have begun to proactively secure their systems at unprecedented levels – a task that is both resource and time-intensive. But smaller organizations, with fewer resources and man-hours to dedicate to proactive security, have not been able take the same precautionary steps. Small organizations are left vulnerable to a wider variety of threats, and are increasingly becoming targets for cybercriminals, hacktivists, and state-sponsored attackers.[2]

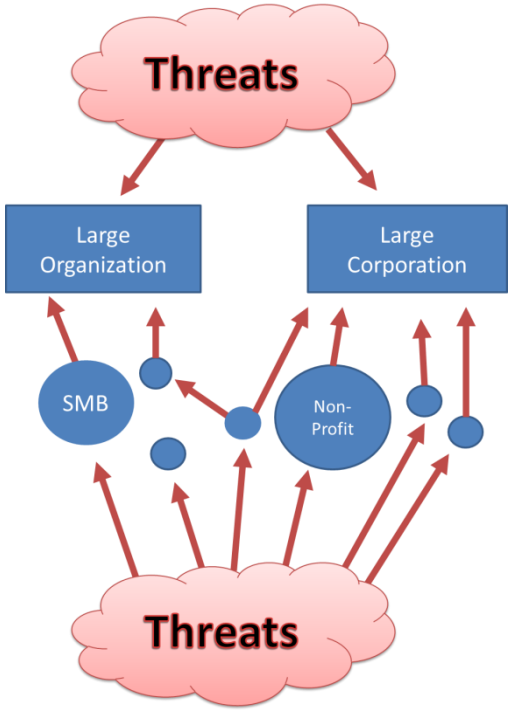

Figure 1: Compromised networks in small organizations can pass threats along to large institutions through partnerships and third-party services

A Wide Array of Attack Vectors

No organization is immune to cyberattacks – but not all defenses are created equal. Some attacks, like those executed by a class of attackers known as "Script Kiddies", come essentially pre-packaged for attackers, and are as predictable as they are blunt. Other, more malicious and sophisticated assaults on information systems might exploit what is called a "Zero Day" vulnerability – one that is previously known to researchers, but exists in an exploitable fashion in a piece of software or hardware's factory or officially-upgraded condition. Just as the nature and motivations of attackers are broad – so are their tools. If no organization can be truly secure, then what is a fair goal to set as a baseline for

[1] A recent GAO report cited a 782% increase in cyberattacks on government agencies from 2006 to 2012. See: "National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented" GAO-13-187. February 2013: http://www.gao.gov/products/GAO-13-187

[2] Verizon recorded 621 confirmed data breaches in 2012. Nearly half of those were at companies with less than 1,000 employees. Twenty percent of those were at companies with less than 100 employees. "The 2013 Data Breach Investigations Report", Verizon Enterprise, April 2013: http://www.verizonenterprise.com/DBIR/2013/

cybersecurity?

Very few standards exist, and none are universally accepted, to describe what makes a system "secure." The "20 Critical Security Controls"[3] or the NIST SP 800-series Special Publications[4] have attempted to provide a baseline, but for organizations without dedicated security teams, the knowledge imparted by these long documents is difficult to digest and turn into tactical knowledge for day-to-day operations. SMBs who operate online need to house credit card and other sensitive data for their customers, and the growth of electronic health records mean your local doctor will soon have to provide secure data services as well. Small organizations, like non-profits, advocacy organizations, and start-ups, are increasingly housing more data of great value. While the motivations for major criminal cyberattacks of the previous decade years have been primarily financial, the age of politically-motivated attacks is upon us. Sensitive information about political and social affiliations, databases of activists, and conversations of a private nature are increasingly becoming targets for attackers.

The Human Resource Problem

In a large organization, a dedicated team of security professionals would serve as the primary line of defense against a changing threat landscape. However, in small organizations, employees in charge of information security are often also in charge of the organization's website, and their database management, and their IT support, and their graphic design – the list can go on and on. There is little time to dedicate to proactive security planning and risk assessment when so much energy of the staff of one or two employees is dedicated to reacting to requests. Often, these technical professionals will be hired for one particular task, and watch their job description quickly creep to include a vast array of responsibilities.

This lack of dedicated security resources makes organizations vulnerable, and not only to sophisticated attackers. IT managers for small organizations can often have little or no information security training, depending on their background, and have little budget to spend on sophisticated tools or expensive hardware that might save them time and energy. Even though some tools are free – like Snort, Wireshark or Maltego – it takes time and training to understand how to use their full capabilities. But where is a small business's budget line for that kind of training?

The Idea

A number of voluntary networks exist between cybersecurity professionals, with a wide range of expertise and capabilities. There are listservs that only allow security staff from particular sectors, or companies above a certain size. These tend to be networks of the elite security experts – those who deal with some of the most sophisticated attacks, and have substantial confidence in those with whom they're sharing information. Constructed primarily around incident response, many of these groups share what are referred to as "indicators," specific evidence of different kinds of attackers or a specific attack. These can include Malware signatures and heuristics, Snort rules, firewall configurations, software whitelists – tactical, easily used information.

There is a pool of information that is available – information that is readily usable to improve information security – but only to a small group. How can small organizations get access to this level of expertise, to this practical and immediately useable information? Unfortunately, one of the elements that make these small groups effective is their size – the listservs are private and trusted. Merely increasing the number of subscribers creates a substantial security problem – the email lists can become targets. The same is true for distributing this information via forums or other

[3] "20 Critical Security Controls Version 4.1" SANS Institute and the Center for Strategic and International Studies" http://www.sans.org/critical-security-controls/

[4] "Special Publications (800 series)", National Institute of Standards and Technology, http://csrc.nist.gov/publications/PubsSPs.html

online presences; any known location of this kind of information will be a target for attackers who will want to exploit knowledge of the private settings of major organizations.

Phase I

In order to overcome trust barriers and effectively and broadly improve information security, we propose a mentorship program between cybersecurity professionals at large establishments and the IT staff at small organizations. The program will pair professionals from large enterprises with technical employees at small organizations based on the skills needed by the smaller entities. Mentors will train mentees in sessions, either in-person or through direct communication (Video chat, screenshare, etc.), twice a month on areas of cybersecurity tailored to the small organization's needs. Mentors will we broken into three classifications:

- **Application Security:** This will likely be the area security training in the highest demand from small organizations. Application security professionals will provide insight into how to develop organizations processes to defend against vulnerabilities in common software (Microsoft Office, Adobe Reader, etc.), as well as strategies, tools, techniques to develop secure web sites and applications.
- **Network Security:** Network security professionals will provide training on tools, strategies, and architectures that prevent intrusions into private networks. This includes organizational and technical policies to prevent unauthorized access to sensitive information, data, or systems.
- **Enterprise Security:** While this will be the least in-demand, mid-sized (in this context, those with more than 50 employees) organizations with a small or growing technical footprint may require substantial assistance building capacity to deal with challenges of securing a distributed network of technical frameworks. Enterprise security mentors will focus on techniques to align security practices across a larger connected workforce.

Potential mentees will register online and describe their organization's security needs, and will be able to see a list of mentors (without names or affiliations) and their skills. Mentors will be able to volunteer through the CDC's website and will be given access to the list of applying organizations. Mentees will be able to select preferred mentors on the site, but ultimately Mentors will be responsible for selecting what organizations they work with. Mentees will be given the opportunity to rate mentors after they have completed consultations.

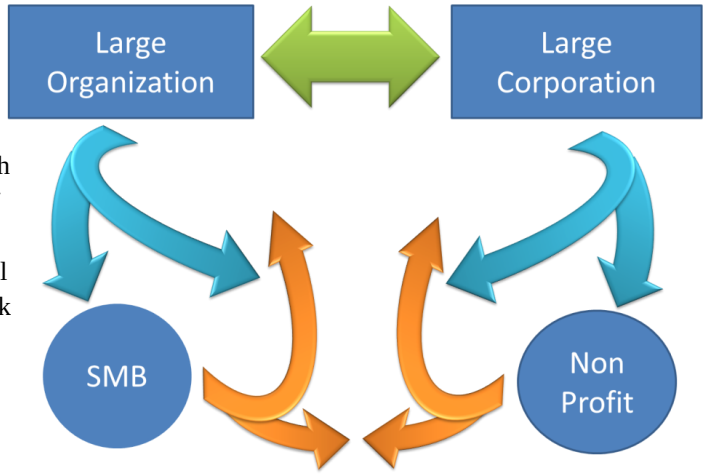

Figure 2: Threat information flows as they exist, and as they will potentially be improved (Phase 1, Phase 2)

Phase II

Once a network of mentors and mentees has worked to improve security and skills, the Coalition will work introduce mentee organizations to their peers in the organization. With a network established, there is substantial potential here to arrange for sophisticated training exercises. The ultimate goal of phase two will be to organize two types of activities:

- **Peer Penetration Testing:** Pen testing, or "red teaming", is a sophisticated audit of an organization's information infrastructure conducted by professionals hired to attack and analyze their systems. The results of these tests often provide distinct recommendations for improvement of security practices and policies,

but this testing often comes at a high price point. Using the peer network built around the mentorship model of CDC as a free pen testing network will provide excellent opportunities for training in advanced security practices, as well as actionable intelligence about organizations' vulnerabilities. The supervision of mentors and the support of participating organizations will facilitate a trusted and safe learning environment.

- **Build a Honey Pot Network:** Honey pots emulate know security holes and are used to collect intelligence about attackers. Information that can be gleaned from honey pots include patterns displayed by malicious web crawling bots and IP addresses of bad actors – information crucial to building effective reputation-based lists for securing organization's IP space. While these traps do not catch brand new attacks, they will provide intelligence to the CDC network – including the larger organizations who serve as mentors.
- **Research Projects:** As a peer network of mentees develops, they could be encouraged to conduct their own security research under the supervision of mentors. The CDC could host code, papers, blog posts, and other projects on its website as a way to promote the work of the mentees and the sophistication of the program.

Even Further

Beyond honey pots is the potential for more sophisticated capture of malicious behavior, software, and intelligence. While the hardware and software for this type of capture can be expensive and difficult to configure, the mentorship coalition will have access to a growing network of professionals who can assist and analyze any information captured. Small organizations who take part in this process will cease to be easy targets, and will instead become valuable sources of new, potentially unseen security data.

Incentives

While the gains for mentees and their organizations are obvious, what is less clear at the incentives for others' involvement. Large organizations will never stop being targets for cybercriminals. But as their security practices have become more sophisticated, so have the attackers' techniques. Small organizations provide a gateway – through partnerships, shared resources, and trusted relationships – into larger entities. Secure systems are only as strong as their weakest link, and unsecure small organizations are a danger to a variety of major entities. Just as it is in the interest of large nations to aid in facilitating the security and stability of the developing world, it is well within the interest of large organizations to lend a hand to small businesses and non-profits. Participating in this coalition e will raise the standards for security practices, and reinforce the barriers to entry of secure systems.

As the CDC progresses, there is also the opportunity to leverage a distributed network of security peers in small organizations to gain insight into threats that may not yet have been seen by larger entities. There is vast potential for collection of new threat intelligence – a substantial motivating factor for organizations beyond contributing to the general stability of online communities.

Development

Mentor Recruitment

As previously mentioned, mentors should come from large organizations and be dedicated cybersecurity professionals. Outreach to these organizations would be primarily to security staff,

but also through public affairs/relations teams. The "sell" to organizations to provide mentors is an appeal to both practical and benevolent instincts: mentorships will improve information security broadly, and may offer an opportunity to collect unique threat intelligence. Similarly, mentorships may provide an opportunity for seasoned professionals to engage with security as teachers for the first time, improving both their conceptual understanding of subjects and their managerial acumen.

There are few large organizations whose professionals could not serve as mentors, but a code of conduct will need to be established and updated to ensure mentors are offering constructive advice. For example, researchers from cybersecurity vendors could make excellent mentors – but there may be conflicts of interest involved in their suggestions of what kind of products should be considered for purchase by mentee organizations. While budgets are small, and it is unlikely their ability to investment in new equipment is limited and should not be abused for private gain.

The mentor community should be well-connected and trusted. New mentors will be vetted by existing members of the CDC, and their organizations should be recognized as strong security practitioners. While this system can begin as an informal network, as the CDC expands it will be important to establish as systematic vetting process. The curation of the mentor list will be the responsibility of CDC leadership.

Costs

While the costs of operating as a mentee in the co-op are variable – expenditures on new equipment and software as new skills are learned, for example – the greatest cost to both mentors and mentees is time. Organizations should view these costs as professional development for mentees, and as opportunities to raise the prestige of mentors in the security community. Initial costs to support the co-op will be dominated by the development of a web platform for registering mentors and mentees. That site's development could be taken in stages:

> **Stage 1:** Development of basic web interface with mentee registration capabilities. Registration will include a basic listing of security needs of that organization, and will be forwarded to the list of mentors. No information about applicants will be stored centrally to avoid security concerns. Web development and hosting for Stage 1 will cost less than $10,000.
>
> **Stage 2:** Mentor feedback mechanisms. This stage would build a feedback system to ensure quality mentorship. This could come in the form of a secure, anonymous/pseudonymous forum or similar system. The goal would be to facilitate conversation about what makes a good mentorship, and establish the effectiveness of mentor consultations. The cost of this system would be variable depending on complexity, but likely not over $5,000.
>
> **Stage 3:** Community architecture development. Depending on the growth of the co-op, this stage could facilitate skill-based, anonymous listings of mentors. It could also include a rating system and a secure registration system that would allow for mentors to access mentee applications through the website. This effort would require a substantial investment in security, and the size of the network would present scaling issues. It is difficult to project these costs – but the co-op would need to be significantly matured and supported in order to bear them.

Funding

Initial funding to get the CDC up and running would be minimal – potentially less than $10,000 to arrange a suitable Stage 1 web site. The money could be raised from a single donor, or in partnership with a sponsoring institution (like a University). Another option would be to source funding from a platform like IndieGoGo, but since the money needed to start the organization is relatively small, it might be worthwhile to wait until a later date to utilize a crowdfunding platform to expand the operations of the CDC.

Long term, the organization will likely be structured as a 503(c) organization, allowing it to be funded primarily by donations. Outreach plans for funding the CDC would include applying for public and private grants, and soliciting private businesses and organizations providing mentors for donations to increase the capabilities of the coalition.

The CDC would also be interested in sourcing in-kind donations of technical equipment from sponsoring entities. Equipment could be potentially stored in physical locations for use and training by mentors, or could be used to support the technical growth of the organization.

Opportunities for Government, Universities, and Certification Organizations

Government cybersecurity is currently a space under significant upheaval and development, and this proposal has focused on non-governmental entities in recognition on the changing landscape for public institutions. However, this model is potentially beneficial for government organizations as well – as state and local governments and sub-agencies are facing the same threats. Government may also be able to improve the incentive framework for participating organizations – though that level of partnership would require significant demonstrated benefits by the work of the CDC.

A barrier to government involvement is the current uncertain legal ground for the sharing of threat information between private and public entities. Recent legislative efforts have made little progress in this area, and while some efforts are underway in the administration to develop frameworks for sharing threat information with the private sector, there is no consensus or precedent for sharing private threat information with the public sector. That barrier recognized – most of the concern in the public sector is about the privacy of customers' data, and not about the strategies for securing information systems. There may be room for government agencies to use this framework while the wider issues of private data are still being resolved.

Universities and Certification organizations could also potentially gain from involvement with this network. By sponsoring training exercises, offering opportunities for joint activities, and accepting participation with the CDC as applicable towards course or recertification hours. Building partnerships between universities and mentee peer-networks will also provide opportunities for more free system auditing. Similarly, mentor organizations will benefit from visibility into working with students for recruiting purposes. The benefits to students are boundless in learning, networking building, and job opportunities.

Measuring Success

Improving cybersecurity can be a difficult thing to measure, since many organizations that are compromised never know they have been attacked. And once an organization's cybersecurity is improved, it is hard to know what attacks would have been successful. Metrics of success will need to be based in the fulfillment of mentee's expectations, and their confidence in their newly-attained skills. As the organization matures, more metrics – including high mentor ratings, the number of multi-organization training exercises, and mentor satisfaction – can be developed, but early measurement should be focused on mentees.