Are the good guys losing the war to cyber criminals? No matter what you believe, it is clear that our trust and confidence in the security of the online ecosystem have eroded and that trust and confidence is the foundation of our Internet-enabled lifestyle. We may be near a tipping point past which people will refrain from connecting to the Internet as the annual costs of being connected outweigh the benefits. Indeed, one recent study predicts that before 2020 the costs of cybersecurity may begin to be greater than the benefits from the information and communication technologies that we rely on (see Figure 1).  

This problem has been in the headlines for years, and has generated a lot of activity by the US government, the information security industry, and many businesses. Much of this activity has been both visionary and diligent. A multitude of laws has been passed to foster privacy and cybersecurity. Private firms continue to develop new security technologies. Spending on cybersecurity has more than doubled since 2009 (see Figure 2). That flood of spending shows no sign of abating.

Yet it remains unclear whether we are winning the battle for security in cyberspace. Clearly throwing money at this problem in the way we have been doing it has been inadequate.

One key element is that the cybersecurity needs of small and medium-sized businesses have largely been ignored. This sector faces challenges that government and large businesses do not. These challenges are difficult, but not unsurmountable. Whether they are addressed successfully will affect the effectiveness of cybersecurity investment. It could help stem the erosion of trust and confidence that our Internet-centered society relies on. That is what this paper will address.

The Cybersecurity Landscape

Three sectors dominate the cybersecurity ecosystem. The US government tries to formulate a national strategy to protect the public and businesses’ cybersecurity with law and enforcement, and spends billions to protect itself. The cybersecurity industry provides the technology and much of the innovation needed to make the ecosystem secure. Large companies have the resources needed to comply with law and regulations, to buy the technology the cybersecurity provides, and to adopt the best practices required to protect their own assets.

The Growing Presence of the SMBs

A fourth sector, small and medium sized businesses (SMBs) has largely been ignored. This sector, composed of businesses with fewer than 500 employees, rivals the other sectors in size. US SMBs employed 56.8 million people, or 48% of the private workforce in 2013. \(^2\)

---

According to one source, SMBs have been the target of 43% of all cyber attacks. In 2016, attacks using email malware and phishing hit them at a greater rate than companies of any other size (see Figure 3).

Yet SMBs are woefully under-protected against cyber attacks. Only 14% of SMBs feel confident that they can adequately mitigate the attacks they face. Adding insult to injury, 60% of small companies go out of business within six months of a cyber attack.

Perhaps most importantly, compromised SMBs pose a formidable negative impact on our society's overall cybersecurity posture. Because the defenses put up by SMBs are inadequate, cybercriminals leverage them to reduce the operating costs of their criminal networks and minimize their risk of getting caught. Some criminals even build their business model on compromised SMBs. For example, criminals can rent botnets made of compromised SMB devices for $67 for 24 hours, or $9 an hour. Waging an attack behind layers of compromised SMB devices makes it extremely challenging for law enforcement and information security professionals to track down the perpetrators because of the prohibitive cost and time needed.

Challenges

The SMB sector faces unique challenges. The firms that make up the sector cannot overcome them individually. These are challenges that need to be approached sector-wide.

First, unlike large businesses, SMBs cannot afford a comprehensive information security program. The components of an effective security program cost time and money that smaller firms often do not have. Creating policies and procedures that address needs specific to a firm, training personnel, evaluating software and vendors, monitoring their networks for intrusions and handling them when they occur all require resources that are hard for SMBs to find. Some of this can be outsourced, but not all. Managed security service providers are expensive, and the cost can easily be prohibitive for firms with small profit margins. Other solutions are readily available on the market, but the prices are higher for smaller firms. For example, personnel awareness training often offers better prices to enterprises with larger employee bases.

---

“SMBs face unique challenges unsurmountable on their own.”

Second, for sustainable security, SMBs have clearly not seen the value of putting time and money into securing their information. Those costs are seen having little value, certainly too little value to justify them. The metrics are simply not there and the hype that surrounds breaches like those of Target and Sony has not been convincing. Those things only happen to the other guy.

Third, this sector has difficulty competing for highly skilled but scarce professionals. Large business and the government can offer higher salary, career development, and favorable benefits. And these professionals do not come cheap. The average annual wage is somewhere around $100,000.00.7

What Can Be Done?

These are significant challenges that call for innovative thinking. It will not be enough for the cybersecurity industry to develop new technology designed for smaller firms. New laws and programs will prove insufficient as well. As is often said, there is no silver bullet.

Instead, this sector needs solutions that are low-cost, high-value, and readily available. They need to be built on two ideas.

First, cybersecurity is everybody’s business. It belongs not just to the technically proficient, but to everyone who uses a computer. After all, the million-bot botnets we have seen have a million pwned computers behind them.

Second, we have to get rid of the idea that nothing can be done. It is often said that any computer can be hacked if the hacker wants to badly enough. True enough. But a similar thing can be said about a thief and the lock on your front door. That doesn’t mean you shouldn’t lock it. In truth, efforts that are simple for most people can help a lot, like choosing long passphrases or keeping your computer patched. Indeed, some of these things, essential to good cyber hygiene, may be easier for smaller firms than the behemoths.

Armed with these two ideas, we can take count of existing resources and focus on gaps. The information needed for good cyber hygiene is plentiful. Businesses can find much of what they need on sites provided by US-CERT, the Small Business Administration (SBA), and others. The gap is in getting SMBs to be aware of it and to believe it is important to make cybersecurity a part of what they do daily, as natural as turning the lights off and locking the door at the end of the day.

A place to start to address the awareness gap would be a community-based approach that makes customers’ voices heard and their choices clear. It would reward SMBs with more customers if they practiced good cyber hygiene, and expose SMBs with poor cyber hygiene. Along with this visibility, all the existing resources are

readily presented to SMBs for free or at cost, such as the regular training programs provided to small businesses by agencies like the SBA and the Small Business Development Center in Maryland, by colleges and universities and by still others. These are places where many would-be entrepreneurs learn about business, including how to get online. All need a cybersecurity component, low-tech and matter of fact. That won’t solve the whole problem for SMBs, but will build a sustainable cybersecurity ecosystem down the road.

If the challenges that SMBs face are addressed, we stand a chance of bringing them out of the crosshairs of cybercriminals. If we get a solid start toward meeting those challenges by empowering SMBs to secure their information, we can spur the adoption of best practices by SMBs, make it harder for criminals to profit from the mistakes that have made their life easy. Then, ultimately, we can stem the slide of the public’s trust and confidence.

About Adaptable Security

Adaptable Security Corp is changing the cybersecurity landscape by strengthening the individual users and organizations. With intuitive security ratings of businesses and products, you have the power to protect your sensitive information at https://adaptablesecurity.org