Cyberattacks Are Crushing SMBs

Christopher Thorpe <cat@post.harvard.edu>
October 2019

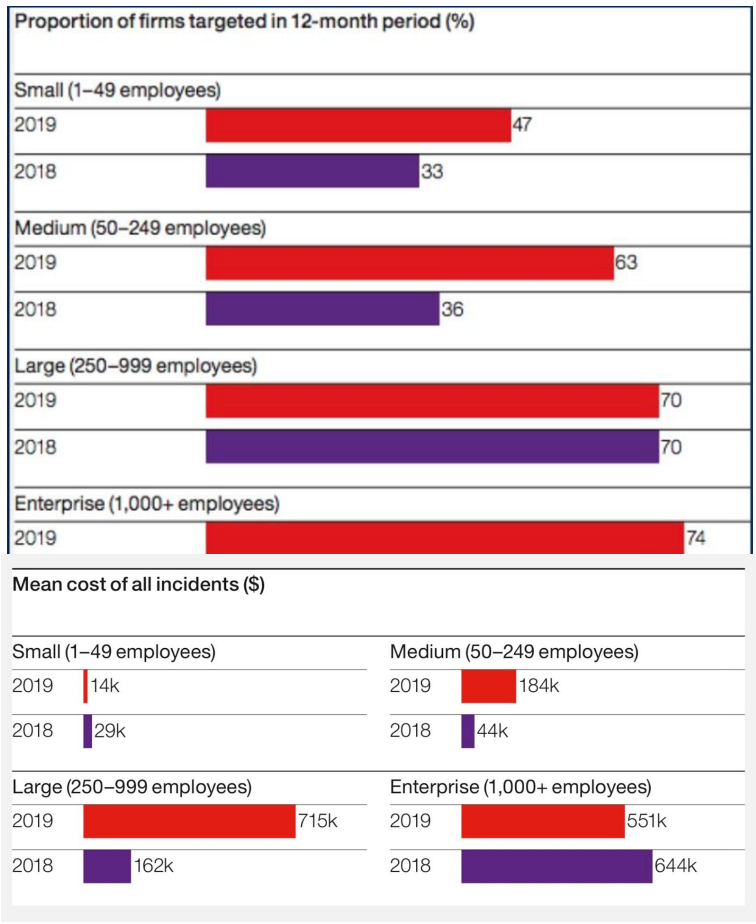
Summary

The explosion of cybersecurity threats and associated costs is crushing small/medium businesses (SMBs). My presentation would describe the situation, explain how they're not being addressed today, and present some ideas for addressing the crisis.

The Problem Is Growing—Fast

According to Hiscox insurance, 2019 was the first year a majority of SMBs reported a cyberattack in the prior 12 months. Cyberattacks are by far the fastest growing cost to small businesses. The number of medium businesses (50-249 people) reporting cyberattacks grew to 63%, an increase of 75% from 2018-2019.

The average cost to medium businesses of cyberattacks grew from $44,000 to $184,000—over four times—in that one year.



Worldwide data, April 2019. Source: https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf

What are the key threats to SMBs?

SMBs need to be most concerned with phishing, ransomware, data theft, vandalism, and botnets. Phishing attacks are most expensive when a business transfers money to a fraudulent recipient; fraudsters often impersonate company executives or attempt to change vendor payment information. Ransomware and vandalism can lock up computers, systems, or data, leading to business interruption. Sometimes the data is permanently lost even if the ransom is paid. Data theft can be expensive because of the liability: people whose

data were stolen need to be notified, and may require the company to pay for credit monitoring. Botnets make computers and networks slow, and create backdoors that increase the risk of other cyberattacks.

Why is this happening now?

1. Enterprises have defended themselves well, and there is less money to be made in attacking them. (Indeed, the Hiscox data shows the average cost of all incidents went *down* for enterprises.)
2. Automated cyberattack technologies are getting cheaper every year. This makes it easy to attack SMBs with phishing, ransomware, malware, botnets, worms, etc.
3. SMBs don't have the expertise to defend themselves, or the money to hire people to defend them. This makes them more efficient targets.
4. The worldwide shortage of cybersecurity professionals means there aren't enough of them to fill the needed positions, and they are too expensive for most SMBs.

What can we do about it?

- User education is important, but it will never be sufficient. The cyberattacks are now too sophisticated. But we need to keep working on user education. The UK CyberEssentials program is a good model.
- Continue to support effective initiatives like the NIST Cyber Security Framework.
- It should be harder for a business to make an accidental, fraudulent payment. Know-Your-Customer tools should be made more widespread to SMBs so that they can securely verify vendor banking data. Payment systems could be made more robust. For example, the Fed Wire system could validate the tax ID of the recipient with the receiving bank, and reject transfers with mismatched tax IDs.
- Internet providers (ISPs) need to do a better job noticing and blocking suspicious traffic in and out of all customer networks. They don't want to do this today because it costs money and may create liability if they fail. Government could support ISPs through subsidies and liability limitations.
- Government, through SBIR, DARPA, and other grants, should promote the development of affordable automated technologies that can protect SMBs and individuals. It should promote technology transfer of defensive cyber technologies from government and large enterprises to help protect businesses of all sizes.
- Cyberinsurance may also be an important tool. regulation that requires insurers to offer policies with reasonable exclusions. SBA regulations requiring SMBs to carry cyberinsurance may reduce business risk and spread costs around; that ecosystem may also promote better cybersecurity practices to reduce insurance premiums.

Christopher Thorpe is a serial entrepreneur and CEO of Brightgate, a cybersecurity startup. He holds a PhD in computer science (cryptography) from Harvard and is a chartered financial analyst (CFA).