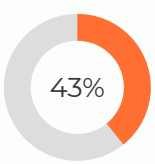
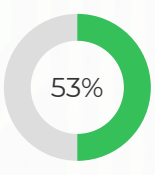
SMB CYBER RISK MANAGEMENT IS ~~HARD~~ NOW SIMPLE

5 Steps Small and Midsize Businesses Can Take to Reduce Exposure

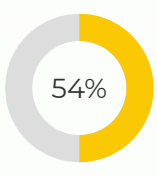
SMBs are in the cross-hairs of cyber-attacks



of cyber-attacks worldwide target small businesses[1].



53% of SMBs have reported a breach[2].



of all cyber-attacks cause financial damages in excess of $500,000[2].

Cyber-attacks on small businesses most often impact the following types of data:

- Passwords or other authentication data
- Payment information
- Software-based products and other copyrighted materials
- The personal data of your customers
- Employee data[3]

SMBs value security, but too many can't afford to improve proactive risk prevention, detection, and response.

Cost and lack of resources is the #1 challenge U.S. SMBs face in adopting cybersecurity best practices[3]. Put another way, SMBs are taking a bare-bones defensive approach against a morphing wave of largely AI-assisted and automated attacks that can discover and crack a static level of protection, creating IT fire-drills that may or may not be effective from an overall organizational damage perspective.

40% The percentage of midsize enterprises don't have a cybersecurity expert[4].

62% The percentage of SMBs don't have cyber insurance[5]. This percentage can range according to how SMBs are defined by size and other factors; a BBB study in the U.S. put this SMB lack of cyber insurance at 85%[3].

If resources were available and affordable, SMBs said they would be likely to:

- Upgrade endpoint security
- Explore better web application security
- Deploy intrusion prevention[2]

5 Steps For Better SMB Cyber Risk Management

Know what you need to protect.

Many SMBs agree that their business is in cyber jeopardy. However, as eager as you may be to take quick action and implement security controls, it's essential that SMBs first understand what is at greatest risk and needs priority protection. A risk assessment is a vital first step to take. When engaging a risk assessment service, keep in mind that you do not want to be left with a massive list of "recommended actions" that may never be realistic to implement, given limited budget and personnel resources.

Shut down suspicious cyber activity sooner.

For many SMBs, remote workers are accessing cloud applications and conducting business outside the visibility and control of the IT and security team. According to the 2019 Verizon Data Breach Investigations Report, 56% of breaches took months or longer to discover. The good news is there are cloud-based security solutions purpose-built for SMBs designed to help them reduce their time to response by consolidating all network traffic and security controls into a single cloud console and enabling SMBs to shut down suspicious activity with a simple click of a mouse.

Insure your business reasonably.

Most SMBs believe they should have adequate cyber insurance, but SMBs sometimes look at cyber insurance as a nebulous thing, which makes it difficult for them to understand what is actually insured and why the cyber insurance policy is of value. Seek out cyber insurance partners that have carved out a program designed to suit the needs of SMBs – such policies should be transparent about the details of coverage and be flexible and affordably priced to help SMBs incorporate this essential component into their risk management program.

Implement flexible security controls that reduce risk scope.

The more security products that are implemented, the more skilled security experts and dollars are needed to manage and maintain them. Cloud-delivered security enables SMBs to implement next-generation security controls affordably in minutes without increasing the burden on IT and security resources. In most cases, cloud-delivered security greatly reduces cyber risk while improving SMB productivity.

Get your incident response plan in place before a crisis occurs.

A key component of an SMB cyber risk management strategy is the design and implementation of a proactive incident response plan. Figuring out the details on the fly is never a good idea when faced with a security incident or breach. Be prepared by incorporating scenario planning, rapid response, damage control, and crisis communications procedures into the plan.

How Can SMBs Do This?

CyberON is a turnkey, affordable cyber risk management program specifically designed to help SMBs immediately achieve a baseline level of cybersecurity.

Learn more at
WWW.PSAFINANCIAL.COM/CYBER-PROTECTION

FOOTNOTES

1) Verizon DBIR 2019: https://enterprise.verizon.com/resources/reports/dbir/?cmp=paid_search:google&gclid=EAIaIQobChMIop2wjYzO4gIV1YuzCh1QPAO2EAAYASAAEgLurvD_BwE

2) Cisco 2018 SMB Cybersecurity Report: https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf

3) Better Business Bureau, 2017 State of Cybersecurity Among Small Businesses in America: https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf

4) Gartner Midsize Enterprise Playlist: Security Actions That Scale: https://www.gartner.com/en/documents/3874970-midsize-enterprise-playlist-security-actions-that-scale

5) Spiceworks 2019: https://www.spiceworks.com/press/releases/spiceworks-study-reveals-nearly-40-percent-of-organizations-have-an-active-cyber-insurance-policy/

PSA INSURANCE & FINANCIAL SERVICES

OPAQ