MANN GROUP CYBERSECURITY

The Value of Cybersecurity for Small Business

Abstract

Organizations understand that fraud exists and they manage the risk, but this due diligence has not kept up with the adoption of technology by small businesses. The volume of critical and private data living in cyberspace has exploded in recent years, but cyberspace itself remains a haven for bad actors that is growing in size daily. This current state of affairs poses major risks, but also opportunities. Cybersecurity investment provides not only risk management, but competitive advantage. As customers grow more concerned and aware of data privacy and stewardship, organizations that have sound cybersecurity can market to customers for competitive advantage over less secure competitors. Customers will abandon service providers who fail to protect their data in favor of those that do. This combination of risk management and competitor differentiation makes a sound case for compelling returns on cybersecurity investment.

The Small Business Threat Landscape

Since the ancient Greeks, merchants of all sizes have had controls in place to prevent and detect traditional fraud, be it from insiders or outsiders. Fraud persists, but the problem is managed via the criminal justice system. Local law enforcement and government have the scope, authority and capability to enforce anti-fraud regulations by arresting and prosecuting criminals. The due diligence by private businesses, with the support of law enforcement and the judiciary, sets an expectation that criminal fraud will often be caught and punished. This keeps traditional fraud under some control because an aspiring fraudster must weigh the risk against the reward.

The Fraud Pyramid illustrates the three prerequisites for fraud:

1. Capability to perpetrate the crime (physically or electronically)
2. Incentive (typically a need for money or desire to cause harm)
3. Favorable risk profile (risk equals the probability of getting caught multiplied by the impact of getting caught)

For traditional fraud, the capability to perpetrate can be reduced through business processes, and the risk profile is not favorable due to the effectiveness of law enforcement; however, cyberspace has a higher capability for fraud but a lower risk profile, and this has resulted in an explosion in cybercrime.

There are three main contributors to the increase in cybercrime in recent years:

1. Ease of deployment
2. Lack of enforcement
3. Geopolitical instability and aggression

Performing a successful cyberattack on a small business in the U.S. has never been difficult for focused threat actors, but it has gotten much easier within the last few years. Cloud or "Software as a Service" (SaaS) providers such as Salesforce provide users with a highly optimized platform managed by a third party at a favorable cost. This business model is now used for "Ransomware as a Service" (RaaS) in the world of cybercrime. An extortionist "customer" subscribes to the service, does the work of building their attacks using the RaaS provider's tools and templates, performs phishing and social engineering and manages the ransoming process. The RaaS cloud service provider offers the tools, templates, guidelines and possible consulting support, then takes a cut of 10-20% of the ransom. This has made the cost and required technical skill capabilities of entry very low for aspiring extortionists.

The scope, authority and enforcement capability for cybercrime is not as clear and mature as traditional fraud. If an employee or thief physically steals money from a business, the proprietor can report them to the local police, who works with the county district attorney to arrest and prosecute, and recover whatever money possible. Cyberspace does not operate this way. The FBI and DHS have jurisdiction for cyberspace, but are challenged dealing with the increasing volume and sophistication of cybercrime. State and local governments struggle to protect themselves from ransomware. Since most serious threat actors are operating outside the U.S., law enforcement's capability to reduce criminal activity through punishment is constrained by resources and jurisdiction.

Cyberwarfare capabilities have been in development by most nation states, but the world has not yet experienced a full-fledged active cyberwar between two nations. With tensions and animosity growing between the U.S. and our traditional foes including Russia, China, North Korea and Iran, the possibility of a warm or hot cyberwar is growing. North Korea, a cash poor and aggressive nation, finances its nuclear weapons program with ransomware attacks on NATO businesses and public institutions.

The world has not experienced unrestricted cyberwar to date, so it is unclear how it would impact non-combatants. However, history shows that new technology changes the nature of warfare profoundly, and when used on the battlefield, changes the world in unpredictable ways.

Cybersecurity as Competitive Advantage

Small businesses have been slow to adopt cybersecurity due to lack of resources, lack of affordable services and misconceptions about the threat facing them. The paradigm is shifting, however. Customers are gradually becoming less tolerant of businesses that appear to be uncaring about protecting private data. Attacks are increasing and becoming more publicized. Regulations and compliance are increasing in scope and enforcement, along with fines for breaches due to willful negligence.

The following predicted trends should be considered when looking at the value proposition for cybersecurity investment by small business:

1. Cyberspace is becoming more regulated, as seen recently in California and the European Union. California's Consumer Protection Act (CCPA) takes effect in January and closely resembles the EU's General Data Protection Regulation (GDPR) which went into effect last year. These regulations place greater restrictions and accountability for protecting consumer data. As the regulatory environment becomes more restrictive with greater enforcement, businesses slow to invest in cybersecurity will struggle to comply, while those who invested will be able to demonstrate and market their mature cybersecurity practices to customers and regulators.
2. Customers will increasingly demand safeguards for their private data. This is likely to be concentrated in the healthcare sector. Patients will make buying decisions based on the trust in the capability of their providers to maintain data security and business continuity. Cybersecurity will be viewed by the healthcare industry and the public as a patient safety issue, not an IT issue.
3. Businesses able to defend themselves from cyberattack will differentiate themselves through pure market forces and time. Small businesses are victims of 43% percent of cybercrimes reported, but only 14% are prepared to deal with an attack, and 60% of victims go out of business within 6 months (Verizon 2018 Data Breach Digest). The punishment for cybersecurity failures is growing, but those who learn and adapt will have opportunity to increase their market share and thrive.

Conclusion

Three factors keep traditional fraud in check but are notably deficient in cyberspace:

1. Barriers to entry for prospective criminals
2. Risk of being caught and punished
3. Stability of environment for doing business

Few barriers to entry, low risk of punishment and an unstable geopolitical environment have raised the cybersecurity threat to U.S. businesses to new heights. Businesses that recognize and respond appropriately to the threat and opportunity will have greater success in the evolving information economy.

As the appetite for cybersecurity security investment by small business grows due to the business drivers identified above, cybersecurity suppliers will improve their capability to fill the need for affordable cybersecurity solutions available to small businesses locally. The majority of talent, products and services are now allocated to medium and large enterprises, but new products and services are evolving to fill the niche and equip small business to protect itself.

Mann Group Cybersecurity provides cybersecurity risk assessments and recommendations to small businesses and public entities in Southern Washington at a low cost.

Learn more at www.manngroupit.com

REFERENCES

Ransomware as a Service (RaaS) article by Forbes:
https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#7fe2b76a4123

North Korea cybercrime funding their nuclear program article by CPO Magazine:
https://www.cpomagazine.com/cyber-security/north-korea-funding-its-wmd-program-with-cybercrime/

2018 Data Breach Digest report by Verizon:
https://enterprise.verizon.com/resources/reports/data-breach-digest/

New America report on healthcare cybersecurity:
https://d1y8sb8igg2f8e.cloudfront.net/documents/Do_No_Harm_2.0_2019-10-16_144807_NhxCEwn.pdf

CCPA and GDPR law comparison:
https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf