
CYBERSECURITY
For Business Owners
HERITAGE
CAPITAL GROUP
BVI
BUSINESS
VALUATION,
INC.

Cybersecurity Defined

> Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

National Institute of Standards and Technology (NIST)

Cybersecurity Defined (Continued)

Cybersecurity includes protecting people, processes, and technologies through confidentiality, integrity, and availability.

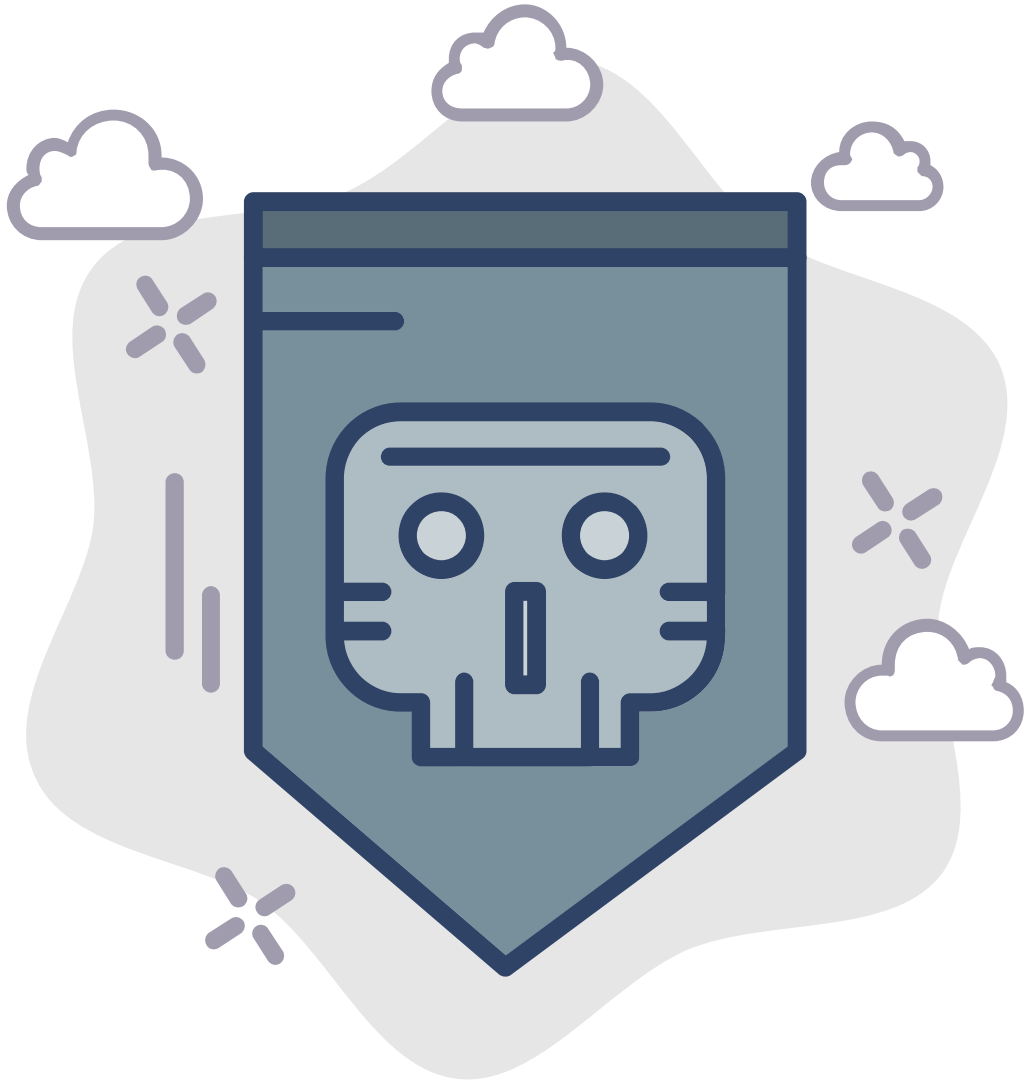
National Institute of Standards and Technology (NIST) further defined cybersecurity as the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation

It’s in the Numbers

According to 2021 Verizon Report

- phishing increased by 11%
- ransomware by 6%.
- Main entry points became accessible through social engineering
- 61% of data breaches were due to credential theft

2021 Data Breach Investigations Report



2021 Recent Attacks

solarwinds

AXA
3 TB of data

Quanta Computer
Apple Supplier

Travelex worldwide money
London Foreign Exchange Firm

Exchange
Microsoft Exchange

CNA
15,000 Devices

acer
Revil $50m

Colonial Pipeline Company

JBS
Meat Packing Company

Robinhood
7m customers

BRENNTAG
Chemical Distribution Company

NBA
500 GB of Confidential data from the Houston Rockets

LOG4J

CD PROJEKT®
Video Game Developer

VSA™ by Kaseya
REvil | 60-80 customers = 800-1500 companies; $70m bitcoin

Microsoft
Print Nightmare

15.5 billion

Johnson & Johnson experiences 15.5 billion cybersecurity incidents on a daily basis. (Becker's Hospital Review)

It's a Global Issue

- **December 2021:** Cybersecurity firms found government-linked hackers from China, Iran, and North Korea attempting to use the Log4j vulnerability to gain access to computer networks - Over 600,000 attempts to exploit the vulnerability.
- **December 2021:** Chinese hackers breached four more U.S. defense and technology firms. The hackers obtained passwords to gain access to the organizations' systems and looked to intercept sensitive communications.
- **November 2021:** A Russian-speaking group targeted the personal information of around 3,500 individuals, including government officials, journalists, and human rights activists. The group obtained access to private email accounts and financial details, and operated malware on Android and Windows devices.
- **November 2021:** Hackers gained access to the social security and driver's license numbers of employees after compromising a U.S. defense contractor.
- **November 2021:** Hackers gained access to the FBI's Law Enforcement Enterprise Portal—a system used to communicate to state and local officials—and sent a warning of a cyberattack in an email claiming to be from the Department of Homeland Security (DHS).

THE WALL STREET JOURNAL.
February 18, 2022

Industry Doesn’t Matter

- Vulnerabilities have led the attack landscape to include strategic industries, such as utilities, healthcare, transportation, and the financial sector

Size Doesn't Matter

Small and medium enterprises (SMEs) are soft targets that can provide the attacker money, information, revenge, or a potential portal to access and attack a larger company.

(Paulsen & Toth, 2016)

Frequency Doesn't Matter

Cybersecurity attacks on SMEs happen exponentially more often and at a higher rate than more prominent organizations that make the national news.

(Aguilar, 2015; Verizon, 2021)

The average cost of an attack on SMEs

(HISCOX, 2021)

$25,612

Do they have your attention?

The Association for Corporate Growth commissioned a survey of more than 300 middle market executives in 2020. “Digital Risk: was cited as the most concerning macro business risk for 2021.

3 Elements For Cybersecurity

TECHNOLOGY

The tools used to protect you

PROCESSES

Rules and guidelines implemented to mitigate risk

PEOPLE

Employee training and support

Small Business Challenges

- Limited technology funding for operational and marketing purposes
- Limited time to focus on cyber
- Limited resources (personnel, capital)
- Cash flow management
- Limited access to cybersecurity talent
- Lack of technical knowledge of leadership
- Organizational culture

$25,612

SMEs were targeted by over 50% of all cyberattacks

Verizon Enterprise (2018)

Increased Opportunity for Hack

- Increase in internet and internet-connected device usage, businesses are more susceptible to cyberattacks than ever before.
- When a business becomes more dependent on the internet, the potential for a cyberattack increases exponentially to the business (Radanliev et al., 2020).

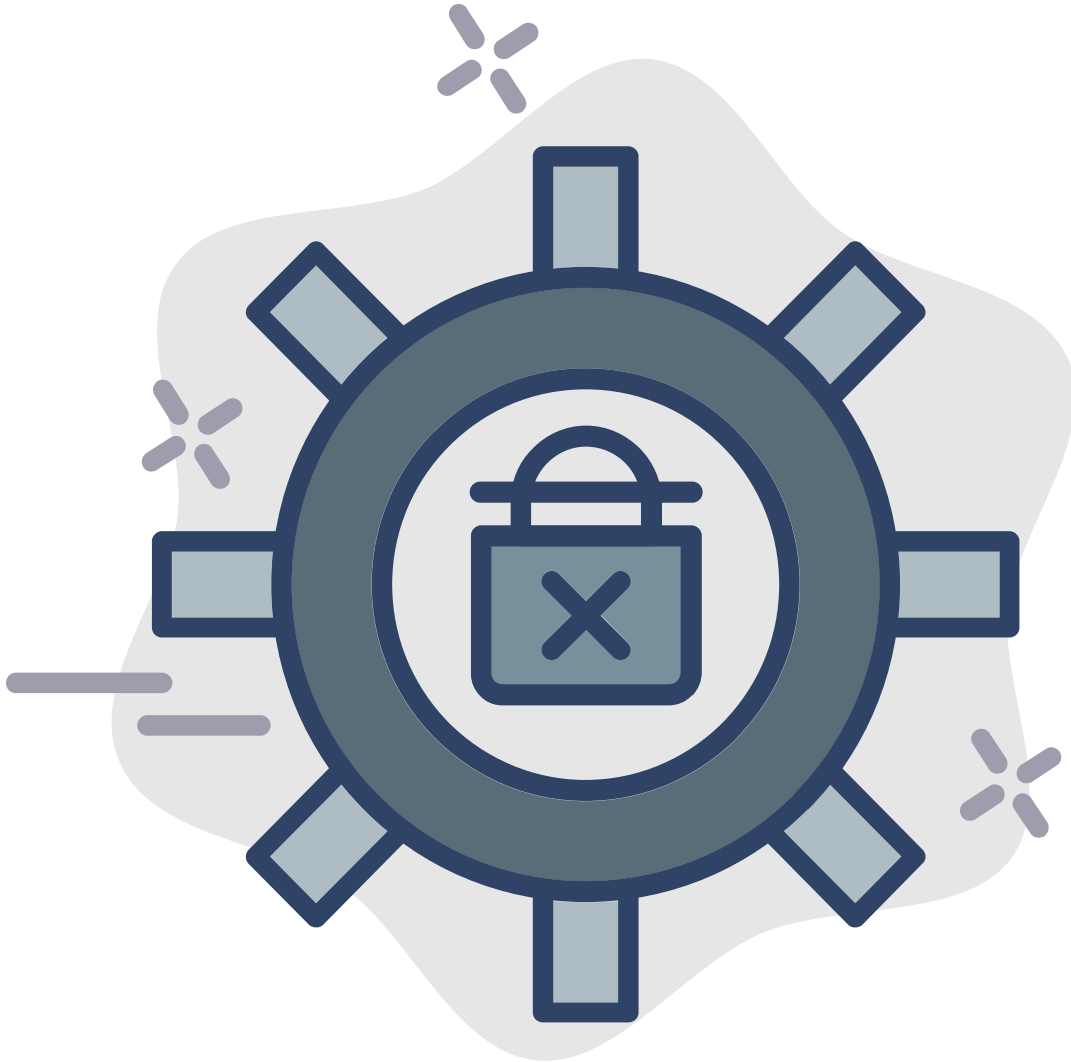
Growth at all Costs!

A Cyber Challenge

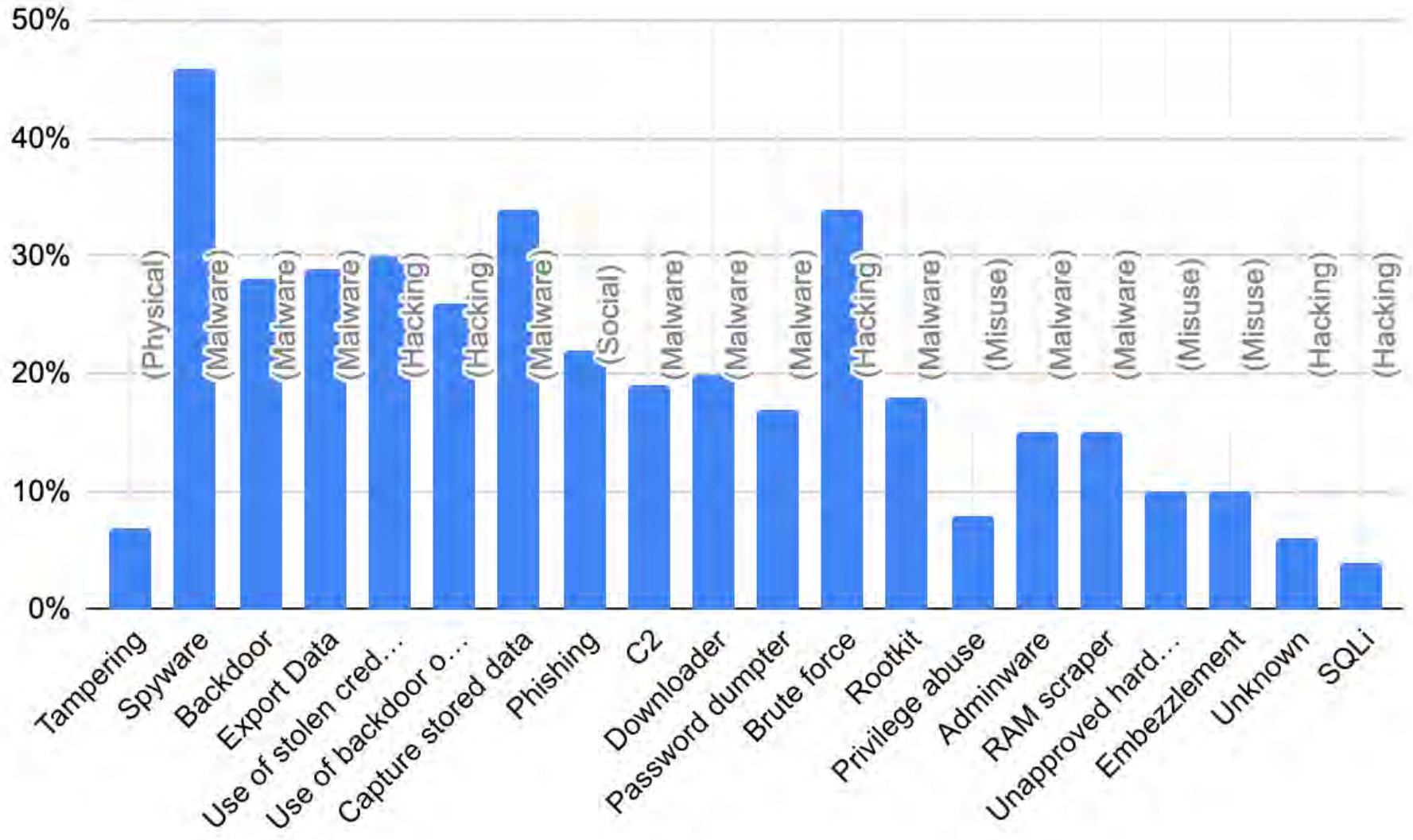
A singular focus on a growth mindset results in leadership neglecting or forgetting other business priorities, especially when it comes to cybersecurity!

Leadership Involvement

Small business leadership involves managing the day-to-day business. Management involves the coordinating of people's behavior, responsibilities in the organization, defining and directing goals, objectives of the company, the people, and the strategy.



"Without the appropriate staff to configure the firewall, route the network traffic flow, and implement a trustworthy design, the firewall is not of much use"



Verizon, 2020

The compromised assets include everything from user POS terminal at 29% to POS terminals from the server at 29%, desktop 24%, laptop 20%, web application 10% and others.

60%

60% go out of business within six months of the attack

(Moschovitis 2018)

Cyber Concerns
Technology

- maintaining a website
- migrating to cloud computing
- E-commerce
- sending and receiving emails

Organizational Culture

- A leader focused on building a cybersecurity culture will prevent the haphazard execution of cyber training, communication, and performance management
- Technology adoption and, importantly, the adoption of cybersecurity within an SME typically falls on the owner or CEO.

Organizational Culture

- Executives and small business CEOs should examine their internal traits, which may increase the odds of technology adoption compared to external traits
- The two most significant traits needed for a technology-driven culture are entrepreneurial mindset and technology readiness
- The leader's ability to take these sources of influence and apply them organizationally is crucial to cybersecurity adoption

A Cybersecurity Culture

> A cybersecurity-driven culture is a combination of technology and investments in the people and processes of an organization

(Huang & Pearlson, 2019)

Best Practice Framework

People	Attract and Retain the Right People
Technology	Focus on Prioritization of Tech Investments
Training	Execute Continuous Training & Monitoring
Culture	Drive a Cybersecurity Organizational Culture
Learning Mindset	Foster A Learning Mindset Beginning With Leadership

5 Biggest Cyber Risks to SME

1. Phishing Attacks
2. Malware Attacks
3. Ransomware
4. Weak Passwords
5. Insider Threats

7 Essential Mitigation Tactics

1. Antivirus
2. Patch Management
3. Email Filtering
4. Web Filtering
5. Admin Privileges
6. Access Control
7. Backups

Do you need a cybersecurity insurance policy?

- Your company handles sensitive information which includes personal health information (PHI) or personal identifiable information (PII)
- You host a public website that interacts with customers and stores login data (including offering a blog)
- You use a 3rd party vendor to manager your database, provide online shopping or is a supplier of goods you sell
- You own or use a website or online application, and rely on the security of your business for your income
- Your staff use their own personal devices (BYOD)
- You don’t have enough money stored to cover the cost of a cyber attack
- Your business relies on confidentiality
- Loss of customer information could result in an invasion of privacy, embarrassment or bullying
- You are a prime target for ransomware or extortion

What kind of coverage do you need?

- Network security coverage
  - Includes cost of data breaches to third parties, theft of IP and sensitive data, ransom demands and network failures
- Privacy liability coverage
  - Less tangible losses and vulnerabilities (human error, theft of devices), costs of breach notifications to affected parties, regulatory fines, crisis management costs and forensic investigation
- Media liability coverage
  - Copyright & trademark infringements, malicious defacement of website and libel

Questions to Ask

- What types of incidents are covered
- What are the deductibles
- Exactly how does the coverage and limits apply to first and third parties?
- Does the policy cover any attacks on your company, including as an unintentional victim, or only those which were targeted directly at you?
- What are the timeframes within which you are covered? Are you covered six years down the line?
- Are any 3rd party vendors, suppliers and business associates you do business with covered?
- What is excluded from the policy (i.e. BYOD)?
- Does the policy cover you globally?
- What kind of response time can you expect in the event of a data breach?
- Will you cyber insurance provider increase your premiums if you ever have to make a claim?
- How do you handle evolving cyber threats?
- What are you responsibilities in this relationship (auditing or compliance obligations)?

Future Considerations

Leadership Mindset

Strategic Goals

Organizational Culture

Audits

Continual Monitoring

Cyber SWOT Analysis

Risk Analysis

Bad Actors

Hacker Tactics

Technology “Status”


Questions

Sources

- NIST Small Business Security Center
- NIST Planning Tools & Workbooks
- NIST Cybersecurity Framework
- Fight Cybercrime
- 2021 Cyberhack Database
- Scam Spotter

FFIEC

Cybersecurity Assessment Tool

https://www.ffiec.gov/pdf/cybersecurity/ffiec_cat_may_2017.pdf

CONSIDERATIONS: Assess Your Vulnerability

Contact Information

Bill Sorenson
BSorenson@HeritgageCapitalGroup.com

HERITAGE
CAPITAL GROUP

Paul Dent
Paul@Surenomics.com

SURENOMICS

Bill Sorenson

Heritage Capital Group

HERITAGE CAPITAL GROUP

Bill Sorenson is a principal with Heritage Capital Group. His primary focus is merger & acquisitions and strategic consulting assignments for clients. Bill leads both sell-side and buy-side assignments for clients seeking to sell or grow their businesses. He also leads Heritage Capital Group's strategic consulting practice. In this capacity, he provides exit planning consulting to clients to ensure both their personal and business goals are met through long-term strategic planning. Bill is a certified expert in lean management and has facilitated over 125 lean-based value enhancement projects resulting in improvements for his clients' processes for marketing and sales, operations, manufacturing, project management, cash flow management, and internal support. In addition, Bill is experienced in providing valuation services. His valuation experience includes over 150 valuations for clients in multiple industries to support transactions, buy/sell agreements, financial reporting, tax filing, and estate planning. Prior to joining Heritage Capital Group, Bill served as a director of management consulting services for an engineering and management services contractor. He also served as a manager for the Supply Chain Optimization team for the consulting division of Deloitte & Touche, LLP, leading consulting projects and serving as manufacturing lead for Enterprise Resource Planning system implementations. Bill began his career in defense contracting and progressed to assistant program manager for a technical service contractor, providing logistics support for multiple U.S. Navy weapon system programs.

Bill is a member of the Board of Seaside Community Charter School, the only public Waldorf charter school in the southeastern United States. He is also a member of the Rotary Club of Jacksonville and will serve as its President for the 2021-2022 Rotary year. Bill is a graduate of the Leadership Jacksonville class of 2015. In 2016, he was appointed to the National Advisory Council for the National Association of Women Business Owners. He's served as a panelist for the Jacksonville Women's Business Center's ATHENAPowerLink® program since 2018. Bill has served as a judge for the annual Manufacturers Association of Florida's Manufacturers of the Year Award since 2011. He received his B.B.A. from Virginia Tech and his M.B.A., with a concentration in operations and management information systems, from Purdue University. He also has Series 79 and Series 63 securities licenses.

Paul Dent

Surenomics

Paul began his career at ADP where he managed and led the staffing and recruiting efforts for the ADP National Accounts Division. Paul comes from a family of early computing pioneers/entrepreneurs who founded Computer Power, the largest mortgage processing company in the world. He later founded Hirease, Inc., a very successful North Carolina based company that performs background screenings for clients in the hiring process.

Paul led the migration from an existing client server commercial software system to a full function, internally developed platform technology, which processes over 100,000 individual transactions a day, while handling all billings and CRM. This system was the catalyst for the growth of the company and had become a highly service-based company that offered cutting edge technology. Paul was also instrumental in the acquisition and integration of several technology add-ons and licenses into the Hirease platform. During Paul's leadership, his companies have been among the INC 500/5000 for 5 years in a row and recognized as the "Best Places To Work" in North Carolina.

Paul and Heidi sold the company in 2014. Paul continues to consult with organization's assisting with their technology strategy and management. Paul sits on the Board of Directors for Welltality Health, where he served as an interim CEO. Paul received a Bachelor of Arts in Political Science from Mercer University and a Master of Science in Cybersecurity from Utica College. When not traveling between the mountains and Pinehurst, North Carolina, Paul enjoys traveling, football, hiking and playing a little golf now and then.

Paul's primary focus is advising individuals, entrepreneurs and business owners in cyber planning, strategic planning with technology and organizational processes.