THE AUGUSTA GROUP

The Small Business problem that must be addressed to secure Federal Government and the global Defence Industry Base (DIB)

Small Business makes up over 99% of US businesses. How do you implement cybersecurity, secure intellectual property (IP) and keep companies competitive in the global marketplace?

August 2021

Andy Watkin-Child, Ted Dziekanowski, Jason Spezzano, Brian McCarthy, Josh Jackson

Executive summary

The United States Federal Government and Small Business America face difficult questions concerning the oversight, assurance, and management of cybersecurity. 99% of companies in the U.S. fall under the category of Small Business and employ over 59 million people (47% of the total workforce), generating 44% of U.S. GDP[1] (Small business manufacturing alone generates around 10% of U.S. GDP), contributing to the tax income of Federal, State, Local and Tribal Governments. Cyber-attacks were once an extreme loss or a 1 in 100-year event for many firms. Now cyber-attacks should be treated as unexpected, if not an expected loss. Small Business is more likely to suffer catastrophic failure from a cyber-attack, as they are least likely to afford the costs of implementing a cyber-risk management program and associated cybersecurity solutions. With the average cost of cyber-attacks more than doubling from $700,000 in 2020 to $1.85 million in 2021, Small Businesses on their own are unlikely to afford the costs of remediation. Especially, at a time when cyber insurance premiums are increasing and further cyber regulation is under review by the Federal Government. The issues around cybersecurity and the management of cyber-risk have created a perfect storm for both Federal Government and Small Business.

A paradigm shift is required by the U.S. Federal Government and Small Business, if cybersecurity and cyber-risk management is to be achieved in line with existing and proposed cyber regulations. Small Businesses might find it challenging to manage cyber-risk, as they are required to implement many cybersecurity practices to secure their balance sheets and their supply chains. The starting point is to establish a 'baseline' of the existing cybersecurity posture of Small Businesses in the U.S. We know this can be achieved with the support of Certified Public Accountants (CPAs) and System and Organization Controls 2 (SoC2) assessments. The American Institute of Certified Public Accountants (AICPA) has created the Trust Services Criteria (TSC) which aligns to COSO and the NIST Cybersecurity Framework (CSF), NIST SP 800–53, ISO 27001 and COBIT 5. By assessing TSC and the suitability for control design and operating effectiveness relevant to the security, availability, or processing integrity of information and systems you can obtain an understanding of the baseline cybersecurity posture of an organization. This provides companies with a clear understanding of the cybersecurity posture helps to identify gaps that need remediation. Also, this creates a baseline cybersecurity assessment for Small Businesses. The funding of which could be through Federal Government offset by tax incentives, tax credits job grants and other financial instruments.

The most significant challenge and cost for Small Businesses are implementing the appropriate number of cybersecurity practices that are necessary to protect Intellectual Property (IP). This IP which is invariably the digital data that the small businesses create, transmit and store to run their company or in support of government contracts. This data is critical to Small Business operations and without securing it from cyberattacks small business are vulnerable to having the data stolen or ransomed, leading to breaches in regulation, loss of federal contracts, cyber remediation costs and potentially closure. Transferring Small Business data and allowing for control inheritance with a cloud under a shared responsibility model, reduces the undue burden of implementing complex and expensive cybersecurity practices. The shared responsibility model ensures that Small Businesses can mitigate some cyber-risk by transferring some of the security controls required to protect their information.

Some of the associated costs of implementing and managing the controls through their migration to the cloud can be incentivized by U.S. Federal Government, offset by tax incentives, tax credits, training grants or other financial instruments. By increasing cloud usage there is the potential to improve oversight of critical infrastructure by the Federal Government.

We will achieve better oversight and assurance of cyber-risk through existing regulated bodies such as the AICPA, and through encouraging the use of cloud inheritance of controls. We believe that this creates the foundations for an affordable, efficient, and effective solution to manage cybersecurity for Small Businesses.

Introduction

Securing any organization from a cyber-attack is a complex process. Creating and implementing a strategy to secure an industry sector comprised of small, medium, and large organizations constructed of nationally and internationally interdependent contractors and subcontractors is difficult. It requires the consideration of corporate size, complexity, and demographics of the market participants before a standard can be applied. The demographics of companies that supply the Federal Government, including the DoDs national and international supply chain is a critical consideration when deploying cybersecurity strategy including CMMC.

Small Business America

The demographics of Small Business America identifies Small Business as a critical driver of the U.S. economy. As of 2018 Small Businesses accounted for 99.9% of companies in the United States, employing approximately 59.9 million people, or around 47.3% of the private sector workforce[2] (Figure 1). They created 1.8 million net new jobs in 2016 from the 30.7 million Small Businesses, with firms employing fewer than 20 people being the most significant net new contributor in the U.S.[1], with firms employing less than 500 people.

Taking the definition of a U.S. Small Business in the manufacturing and mining sector is an organization that has less than 500 employees[3]. In 2019 Small Business manufacturing firms accounted for 44% of the 11 million manufacturing jobs in the U.S. (Figure 2). The National Association of Manufacturers (NAM)[4], which represents 14,000 member companies estimated that U.S. manufacturing increased employment by 53,000 in March 2020 taking the total employed in the sector to 12.28 million. This sector increased its value-added output from $2.348 Trillion in the fourth quarter of 2020[3] to $2.44 Trillion in the first quarter 2021, contributing to over 10% of U.S. GDP in 2020. (Bureau of Economic Analysis, U.S. Department of Commerce[5]).

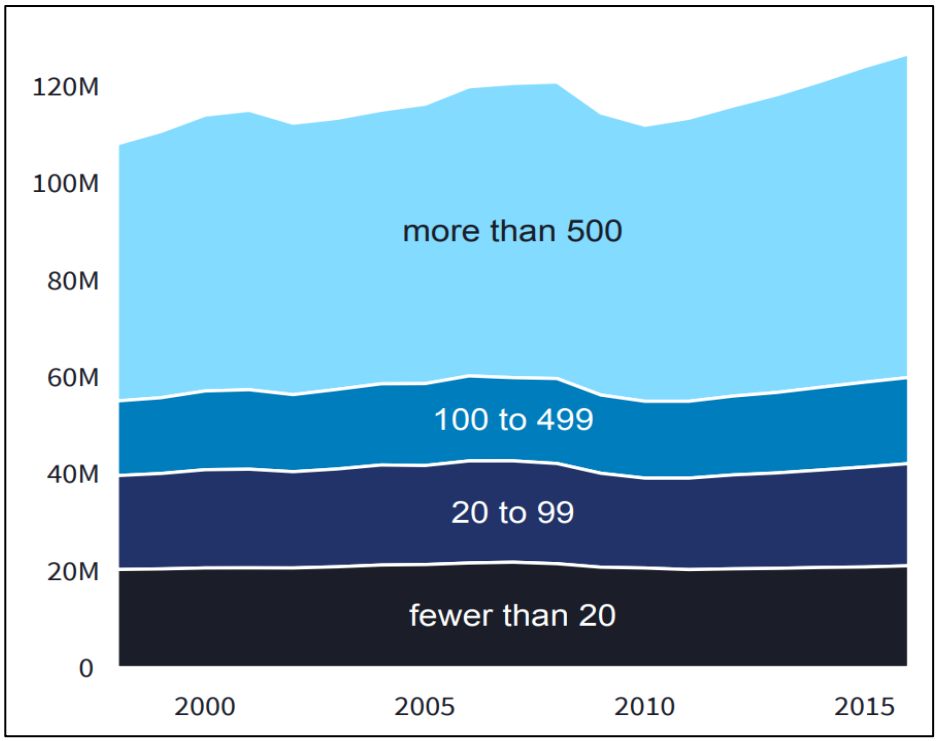


Figure 1: Employment by business size.

This makes the manufacturing industry a critical contributor to U.S. employment, exports, and prosperity.

The DoDs dependence on Small Business America

The DoD Defence Industry Base (DIB) is critical for delivering products and services to fulfil the objectives of DoDs mission. With Small Businesses making up 99.9% of U.S. companies. The DoD and its prime contractors rely on Small Business America to deliver the products and services required to support front-line fighting forces and the DoDs mission. U.S. manufacturers perform 61.8% (NAM statistic) of all private-sector R&D, driving more innovation than any other sector (Bureau of Economic Analysis). With 97.5% of all identified exporters being Small Businesses.

In November 2020 Amy Murray, OUSD A&S Deputy Director Industrial policy said[6]

"Small Businesses are the backbone of the American economy……..Small Businesses are key to DoD's mission and innovation initiatives, their agility delivers the speed and performance to transform the defense industrial base and provide competitive advantage. And this agility drives ... value faster by increasing innovation, responsiveness, customer satisfaction, productivity and quality…..Small Businesses produce 16.5 times more patents than large patenting firms and create more than half of non-farm private gross domestic product, which is significant to our economy……we need to ensure companies can stay in business without losing their precious intellectual property, the foundation of so many critical technologies".

In 2019 the DoD awarded over $75Billion in prime contracts to Small Businesses representing 67% of the companies awarded contracts in the DoD[6].

Small Business Employment by Industry and Self-Employment by County

Industry	Small Business Employment	Total Private Employment	% Small Business Employment Share
Health Care and Social Assistance	8,827,665	19,735,708	44.7
Accommodation and Food Services	8,311,349	13,704,017	60.6
Retail Trade	5,578,660	15,967,893	34.9
Construction	5,196,519	6,311,264	82.3
Professional, Scientific, and Technical Services	5,182,179	8,799,893	58.9
Manufacturing	5,108,012	11,590,420	44.1
Other Services (except Public Administration)	4,689,910	5,499,244	85.3
Administrative, Support, and Waste Management	3,690,079	11,628,509	31.7
Wholesale Trade	3,446,199	6,110,748	56.4
Finance and Insurance	1,920,108	6,336,795	30.3
Transportation and Warehousing	1,667,017	4,729,709	35.2
Educational Services	1,630,541	3,677,275	44.3
Real Estate and Rental and Leasing	1,434,649	2,111,418	67.9
Arts, Entertainment, and Recreation	1,411,192	2,311,437	61.1
Information	906,836	3,447,950	26.3
Management of Companies and Enterprises	401,312	3,380,437	11.9
Mining, Quarrying, and Oil and Gas Extraction	244,160	587,017	41.6
Agriculture, Forestry, and Fishing and Hunting	134,578	160,411	83.9
Utilities	111,076	638,917	17.4
Industries not classified	23,176	23,176	100.0
Total	**59,915,217**	**126,752,238**	**47.3**

Figure 2: U.S. Employment by industry 2016 (US Small Business Administration)

While these figures relate specifically to the U.S. National DIB, the international DIB is vital to the DoD with long global supply chains, made up of prime contractors and subcontractors.

These supply chains can be fragile, as highlighted by the GAO report on 'F-35 Aircraft Sustainment, DoD Needs to Address Substantial Supply Chain Challenges' (2019)[7] and impacting a substantial DoD weapons program. The F35 program was under increased stress due to the lack of availability of spare parts, from across its global supply chain. Due to shortages, F-35 aircraft could not fly nearly 30 percent of the time between May and November 2018. With a DOD repair backlog of about 4,300 F-35 parts impacting mission performance, the F35 Supply chain is an example of global manufacturing collaboration across the DoDs DIB. With suppliers from 45 U.S. states, ten countries and over 1,500 contractors participating in the design, development, manufacture, and servicing of the aircraft. This creates complex challenges for the DoD in ensuring that spare parts and finished airframes are delivered on time to keep the fleet airborne. Challenges which cyber-attacks can exacerbate on the DIB, and highlighted by the various GAO reports[8-13].

Cyber-attacks have been recognized by the DoD as a significant issue, impacting the security of DoD weapons systems and the security of its Defence Industry Base (DIB) and the DIB is made up predominantly of small companies. The U.S. Government Accountability Office (GAO) and Office of the DoD Inspector General (DoD IG) have highlighted the challenges faced by the Department of Defense (DoD) in securing its Intellectual Property (IP). Identifying failures to embed cybersecurity across the DIB, manage weapon system vulnerabilities and protect DoD weapon systems from Cyber-attack[8-13], raising concerns within Federal Government that the DoD and DIB are subsidizing other Nation States create their own weapon systems.

The US is moving rapidly ahead with cyber regulation, to include Supply Chain Risk Management (SCRM). Much of this is powered by President Bidens recent Executive Orders were signed in February and May 2021, respectively. Regulation established now enables the Securities and Exchange Commission (SEC) oversight of Environmental, Social and Governance (ESG) material risks of publicly traded firms in the U.S.. This is highly likely to include oversight of cybersecurity as a material risk, in addition to the assessment of financial materiality under Sarbanes Oxley (Sox) and other industry-specific regulations. The DoD is moving ahead with its CMMC program, releasing an interim final ruling in November 2020, pending a final ruling due in Quarter 4 2021. The current ruling requires all companies that must comply with DFARS 252.204-7012 to report their compliance status of the 110 NIST SP 800-171 cybersecurity practices, to the DoDs Supplier Performance Risk System (SPRS). With an expectation that CMMC levels will be added to DoD contracts from 2021, this is placing an additional burden on Small Business manufacturing. The cost of federal regulations already falls disproportionately on small business manufacturers. Manufacturers pay $19,564 per employee on average to comply with federal regulations. In addition, small manufacturers with fewer than 50 employees spend 2.5 times the amount of large manufacturers. Environmental regulations currently account for 90% of the difference in compliance costs between manufacturers and the average firm[1].

Cyber is no longer a once in 100-year event. It is here and now.

The cyber-risk paradigm through which the DoD, Federal Government and Small Businesses needs to view cyber is constantly changing. Cyber-related incidents were once 100-year events, and they are now a regular occurrence. Where they would once have been considered an extreme loss event, over the past 10 years cyber-attacks have increased in number, complexity, and severity. The likelihood of a cyber-attack is much closer to '1' than '0' (probability of 1, it will happen). Cyber is a risk which Small Businesses cannot ignore.

Cyber has moved from an **extreme loss** to an **unexpected loss** and closer to an **expected loss** event over the past ten years (Figure 3). This is an issue the cyber insurance industry is coming to terms with. Cyber-risk is a hard risk to mitigate for many organizations, due to the lack of cyber-skilled resources and an appropriate controls environment. The cost of cyber-risk remediation is increasing, budgeting for **expected losses** is difficult and the costs of remediating **unexpected loss** are increasing (cyber insurance, capital holding). As the demand for skilled resources increases, the cyber insurance market tightens, the cost and complexity of implementing cybersecurity practices increases (Implementing 110 NIST SP 800-171 practices). Small Business is caught in a cost spiral it cannot manage.

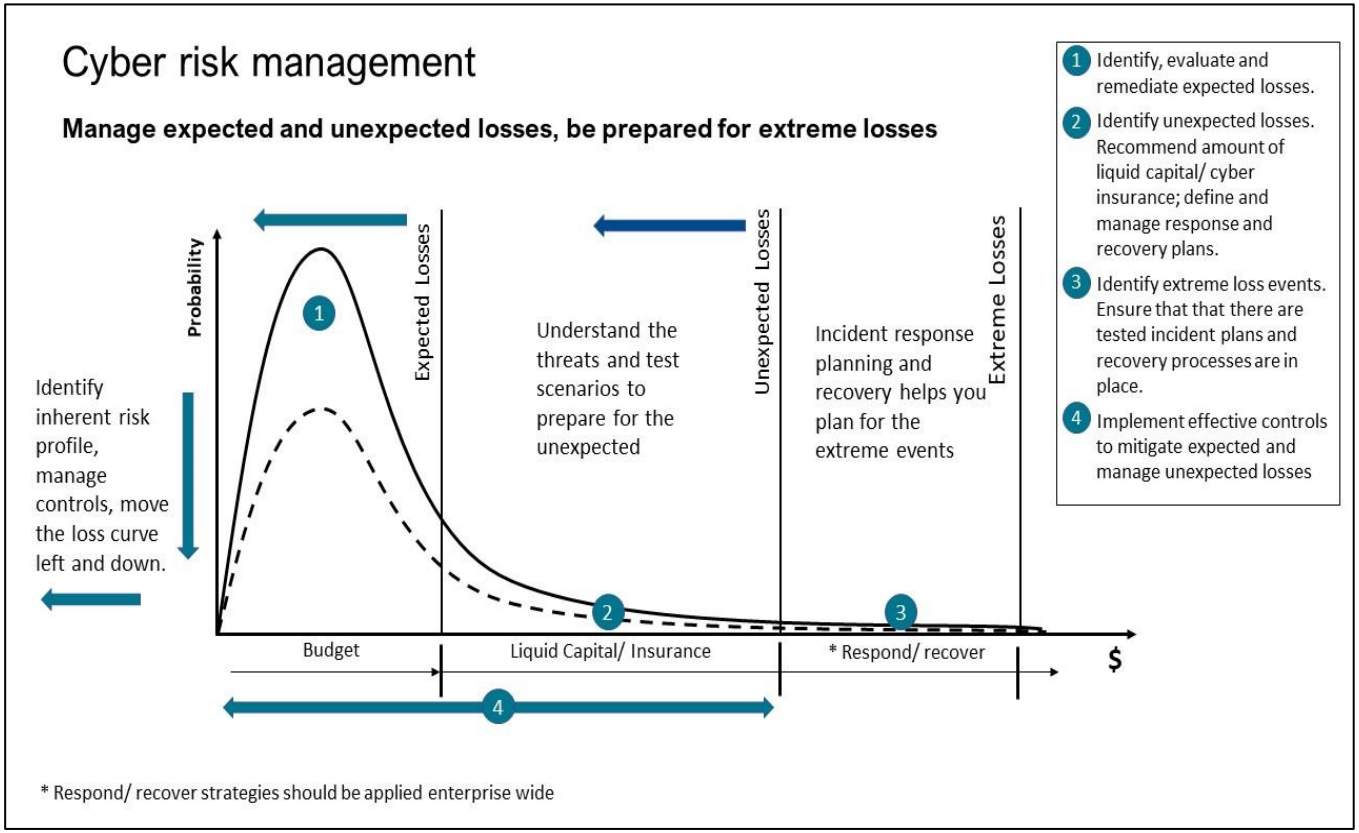


Figure 3: Cyber-risk managing expected and unexpected losses. Planning for extreme losses.

The transformation of cyber-risk from an **extreme loss** to an **expected loss** event creates a significant issue for Small Business. The complexity of global supply chains and the interdependence of organizations down multiple tiers of supply makes it difficult for companies to know where and when a cyber-attack will originate and the impact on the delivery of its products and services. Mitigating cyber-risk by setting aside funds (Liquid Capital) to manage cyber incidents is difficult for Small Business. Placing a reliance on cyber insurance. It is even more complex when the attack originates from within its supply chain i.e. NotPetya, SolarWinds, JBS, Colonial Pipeline and Kaseya. This in turn, places a burden on the insurance industry, which must manage silent cyber losses.

Traditionally cybersecurity has been a difficult proposition to sell in the board room. The costs of implementing of cybersecurity solutions vs. the visible rewards make most CEOs, CFOs and boards take very deep breadths when confronted with any Return on Investment (RoI) conversation. The "it won't happen to me" argument has been well tested in the board room, delivering the expected outcomes. Unfortunately for the Small Business leaders, cyber is an expected loss requiring a quick solution.

Whether boards agree or not, cybersecurity and the protection of corporate information and data, no matter the company's size, is a cost of doing business requiring the management of the corporate cyber-risk profile. Cyber-risk is a prevalent risk and requires solutions that Small Business and the Federal Government need to implement. For an organization to manage cyber-risk it must understand the risk which cyber presents to its balance sheet in line with its appetite to manage the risk. It must identify its inherent risk profile, assess cyber control design and effectiveness to mitigate the risk, and calculate its residual risk.

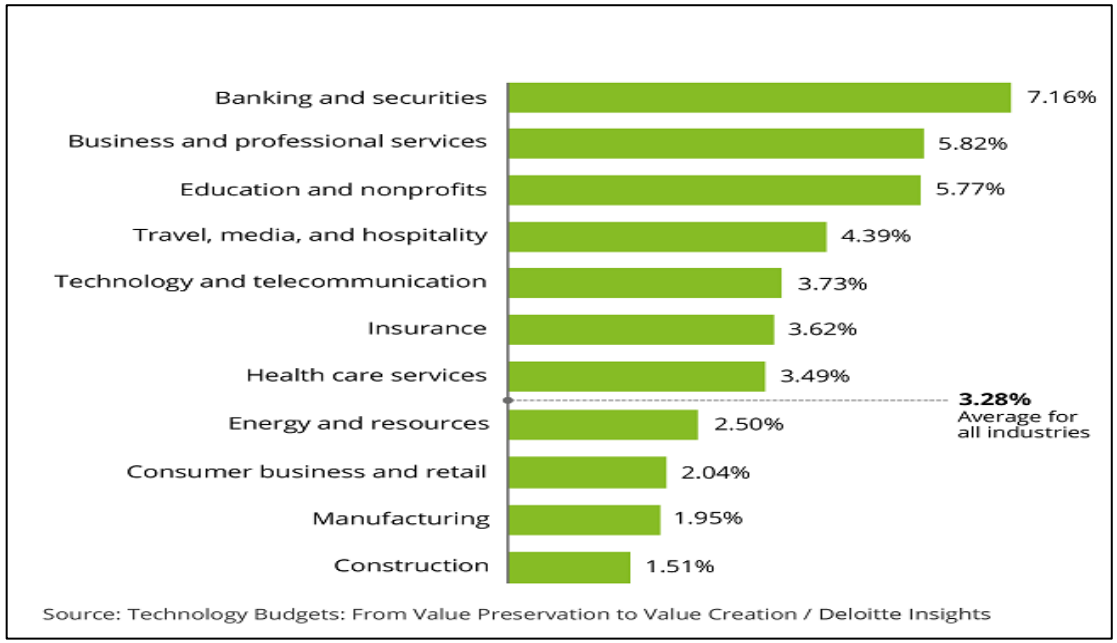
Cyber is an expensive risk to manage

How much do you spend to mitigate cybersecurity risk is not an easy question to answer, for large or small companies? Cyber-risk is an enterprise-wide risk; as broad and as deep as the data which an organization creates, processes, stores or transmits. It is as large as an organization's digital perimeter; as complex as the products and services it manufactures and supplies, the number of people it employs, IT assets it uses, its dependence on digital and the maturity of the cyber threat it faces, be that nation-state, cybercriminal, hacktivist, or script kiddie. Its impact depends on the size of the balance sheet, its cyber posture, the research the threat actor has completed on the organization and the regulatory environment in which the organization operates.

Cyber criminals will invariably go where there is an opportunity to disrupt and make money. Nation state-actors target national infrastructure, Government assets, services, and the private sector where they steal valuable data, which in the digital world is readily accessible Intellectual Property (IP). Many reports detail the impact of cyberattacks, drawing conclusions about the cost of cyber compliance, the cost per record stolen or the average costs of a cyber-attack, which do not convey the real impact of cyber-attacks for small business. The impact of a cyber-attack is as unique to each organization as its data, assets, processes, products, services, markets, and cyber maturity, requiring a solution that is unique to the company.

Budgeting the actual amount of cyber spend for a Small Business is difficult and annual reports and public financial statements do not explicitly identify cybersecurity spend. Therefore, using the generally accepted measure of IT spend (which traditionally includes cyber) as a percentage of revenue as a proxy, the average IT spend for all industries is approximately 3.28% (2017 - Figure 4) of revenue on IT and the average cyber spend is around 10% of IT spend.

On average the top 10 financial institutions each spent on $375Mn on cybersecurity in 2019



One of the most mature industry sectors for technology and cyber spend is Financial Services. Deloitte estimated that on average in 2020, Financial Institutions spent 10.9% of their IT budgets, around $2,691 per employee or 0.48% of revenue on cybersecurity[14/15]. In 2019 The Bank of America spent $10 billion (2019) on Technology[16] and JP Morgan spent $600 million (2019) on cybersecurity[17].

This is driven by factors including regulation i.e. Basel II and the simple fact that banks experience 300 times more cyber-attacks than other companies[18]. Implementing cybersecurity practices such as the NIST Cybersecurity Framework (CSF), complying with the same cyber requirements required by the DoDs CMMC program (Table 1).

Figure 4: IT Spend as a Percentage of Revenue – Wall Street Journal, Deloitte 2017[13]

CMMC Level	Security Practices	CMMC Practices	Maturity Processes	Regulation/ Standard
1	15	-	1	FAR 52.204–21
2	65	7	2	NIST SP 800–171
3	110	20	3	NIST SP 800–171
4	110	46	4	NIST SP 800–171
5	110	61	5	NIST SP 800–171

Table 1: CMMC (including NIST SP 800-171) Cybersecurity practices and levels

The cost of cyber compliance is not small. The NIST SP 800-171A19 document created by the Defence Contract Management Agency (DCMA) and referenced by the DoD in their CMMC interim final ruling (November 2020) as the assessment standards for cybersecurity. It Identifies 320 assessment objectives which must be fulfilled and over 300 individual artifacts referenced including policies procedures and data related documents. Small Business defense contractors will find it very difficult and expensive to implement, oversight and assure NIST SP 800-171 cybersecurity without Federal support.

How can Small Business America manage the risk?

Cyber-risk is too complex for Small Businesses to manage alone. Frameworks such as ISO 27001, NIST SP 800-53 or NIST SP 800-171 define a comprehensive set of controls for data protection, however, any organization that must implement 110 cybersecurity practices, create, and maintain over 300 artifacts requires the investment of a considerable amount of capital in resources, skills, and technological solutions. In general Small Business America does not have these resources.

The Federal Government faces a similar situation. Cyber-attacks create a significant risk to the U.S. economy, and Small Business is a significant contributor to U.S. growth, job creation and innovation. Any strategy for cyber-risk management must reflect this and maintain national security. This requires an approach that innovates the oversight and assurance of cyber-risk across Small Business. By providing the appropriate tools, training, oversight, and assurance of cyber-risk for the Federal Government, the U.S. supply chain and larger companies that also rely on Small Business to fulfil their supply chain commitments can mitigate this risk. We believe this requires the support of the Federal Government.

Oversight and assurance.

Many organizations do not know their cybersecurity posture, how well they manage cybersecurity, or the most cost-effective way to manage their cybersecurity profile. A solution is available to provide small companies with a view of their current cybersecurity maturity, to support the creation of a suitable plan of action and milestones (POAM), to help manage cyber-risk and provide an annual attestation as to their progress towards compliance.

The American Institute of Certified Public Accountants (AICPA) whose member oversight frameworks such as Sarbanes Oxley, created the Trust Services Criteria aligned to COSO and assessed using System and Organization Control (SoC)[20] 1 and 2 reporting. The methodology applied by AICPA is already proven and can be used to assess alternate information types required by other federal agencies. The assessments are prepared by independent Certified Public Accountants (CPAs) skilled in auditing processes and cyber/ IT security. SOC reports reduce compliance burdens by providing one report that addresses the shared needs of multiple users. There are thousands of qualified CPAs that perform SOC audits, giving immediate scale to a global challenge, with reciprocity built-in. While they are not all cyber experts, they are regulated financial audit professionals who have relationships with Small Businesses, attesting annually to the financial statements and compliance of Small Businesses across the US.

SoC 2 assessments have been created to meet the needs of a broad range of users that need detailed information and assurance about the controls relevant to security, availability, and processing integrity of the systems the service organization uses to process users' data and the confidentiality and privacy of the information processed by these systems.

These reports can play an essential role in:

- Oversight of the organization.
- Vendor management programs.
- Internal corporate governance and risk management processes.
- Regulatory oversight.

No magic bullet 1, but a way forward. The Federal Government needs to have a level of assurance that Small Business America can manage cybersecurity, as self-attestation has proven not to be effective as a solution (The DoD implementation of NIST SP 800-171 by defense Contractors). The most appropriate approach is to request companies complete an assessment of their cybersecurity compliance, to an appropriate cybersecurity framework profile, using CPAs and SoC 2 assessments. By performing an initial "baseline" assessment of compliance in year 1, businesses will identify their cybersecurity posture and a plan of action to remediate identified gaps. Subsequent annual assessments will continually identify gaps over the following years, creating a continuous improvement model. This approach provides the mechanism to drive oversight and assurance of Small Business, which can be supported by the Federal Government.

Options for the Federal Government

- They can request that an assessment of cybersecurity posture is completed by the existing community of CPAs annually.
- They can provide appropriate tax incentives to Small Businesses to complete CPA assessments, which will reduce the burden and overhead to the CPAs clients.
- They can provide financial solutions and support training initiatives to up-skill more CPAs to conduct SoC 2 assessments to deal with data types and system they may not be familiar with e.g. cloud.
- They could collate the evaluation results, providing a clear picture of the cybersecurity posture of Small Businesses and critical infrastructure to the Department of Home and Security (DHS).

Benefits for Small Business and Federal Government. While there is no magic bullet, it is a solution that can be quickly applied across Small Business America. This plan provides a baseline assessment and forward-looking plan of action and milestone (POAM) for Small Businesses to implement cybersecurity. Based upon a level of risk agreed between buyers and sellers of products and services, who want to evaluate the cybersecurity risk profile of each other's business for the benefit of trade. Assessed by a trusted advisor, who has a relationship with the firms and is regulated by an appropriate regulatory body. The approach supports international reciprocity, delivered through international agreements between the global accounting professional associations. Addressing issues with existing cybersecurity programmes and supporting the international DIB given the dependence on global supply chains cannot be underestimated.

Such an approach would allow the Federal Government to phase in a solution for the oversight and assurance of Small Business cybersecurity, enabling Small Businesses to understand their cybersecurity posture and make risk-based decisions. This risk-based approach will help Small

Businesses make critical decisions about their current business relationships, customers and suppliers. This can be achieved while being supported by the Federal Government through tax credits, incentives and other funding mechanisms such as grants, and Centers of Excellence.

This approach would also support the training and education of cybersecurity professionals, to achieve an appropriate cybersecurity posture and facilitate the timely oversight and assurance of an appropriate proper cybersecurity framework profile, in line with a SoC 2 assessment.

Control inheritance and data custody.

The most significant barrier for entry for Small Business to manage cybersecurity is cost. Complying with a full scope of cybersecurity standards such as NIST SP 800-171 and CMMC, is prohibitive for many firms. The costs associated with implementing the numerous cybersecurity practices, managing oversight and assurance, reporting and remediation in the event of a cyber-attack is significant, whether as a percentage of revenue, a cost per data record or a cost per employee it creates a substantial burden for Small Business.

Cyber-attacks also cost Small Business. The average costs of cyber-attacks have increased significantly over the past 2-years, with Ransomware being the most significant cyber threat vector. The average cost of a cyber-attack has risen to $1.85 Million in 2021 from $700,000 in 2020[20]. In addition, the price of cyber insurance, the predominant mechanism for risk transfer for Small Business to address unexpected losses, has risen over the past year. Spiking 32% higher between June 2020 and June 2021. Cyber insurance claims are up, capacity is down, and the insurance industry is under pressure[20].

This situation requires a radical rethink of cybersecurity for Small Business. If businesses do not have the skills, resources, or funding to address cybersecurity and manage the risk, what options are available. With all risk management programs there are options.

Option 1: Avoid the risk.

Option 2: Accept the risk.

Option 3: Manage the risk.

Option 4: Transferring risk (through contracts, services, and cyber insurance)

Option 1 is not viable for some Small Businesses, as they are reliant on Federal Government for business and Federal Government is also reliant on Small Business for products and services. If companies accept their cyber-risks, they accept the associated costs of compliance and remediation, and they cannot accept risk on behalf of the Federal Government, making option 2 unviable.

If Small Business chooses to manage all or some of the risk, they accept that they must implement the appropriate controls and practices to mitigate the risks. For Small Business this is a cost they generally cannot afford, making option 3 difficult for many Small Businesses to achieve. They don't have the skills or resources available.

Option 4: is the only viable option for most Small Businesses, procuring cyber insurance is currently a viable option, but prices are rising fast impacting affordability, and companies run the risk that not all costs will be covered, such as fines. An alternate solution is to host critical data in the cloud and transfer some or all of the cybersecurity risk through contracts to a cloud provider. Small Businesses own the data consumed for the creation, sale, and servicing of their products and services and those of their clients. While the security of this data requires implementing a significant number of controls, which are costly to implement and manage, not all controls have to be owned and managed by the Small Business to secure its data. By placing the appropriate data within a cloud environment, the Small Business can transfer some of the cybersecurity risk, required to protect information and data to the cloud provider through controls inheritance, reducing the overhead of implementing and managing some controls. While not all controls can be managed through control inheritance, this approach will reduce the cost of cybersecurity, and will simplify cyber oversight, assurance, and compliance.

The Federal Government can incentivize Small Business and cloud providers to transfer data from Small Businesses to the cloud. Cloud providers already deliver a range of solutions that can be integrated into Small Business operations to meet their needs. The Federal Government could create a list of cloud-based providers, which deliver approved secure cloud applications, storage which are and attested annually by CPAs. Accelerating this approach, cloud providers already assess their System and Organization Controls (SOC 2)[21].

To conclude

The Federal Government has learned many cybersecurity lessons. The recent spate of cyber-attacks has demonstrated that cyber is not an extreme loss by likelihood, but is an expected loss by likelihood and impact. Cyber is a risk that cannot be ignored. It is a risk that will take time to remediate effectively across the Federal Government and Small Business America. The complexity of cybersecurity makes it an expensive risk to manage, and the cybersecurity frameworks and standards in the market today do not fit well with the need for Small Businesses to secure their balance sheet, while maintaining shareholder value. The latest threats such as Ransomware have a devastating impact on companies that are not prepared to manage the risk. Even those who are prepared must endure the costs of incident response and remediation. Cyber insurance has been the ideal risk transfer tool for managing the risk, but the cyber insurance industry struggles to keep pace with the risk[22]. A ransomware attack can be catastrophic, bringing a business to its knees for a significant period of time, impacting companies up and down supply chains.

In 2019 the DoD awarded over $75Billion in prime contracts to Small Businesses, representing 67% of the companies' awarded contracts by the DoD[6], benefiting Small Businesses, their respective supply chain ecosystems, and the U.S. economy. With Federal regulations falling disproportionally on Small Businesses including manufacturers, cyber regulation will add to the regulatory burden and add the cost of doing business. If reasonable and cost-effective solutions can be implemented to protect IP and data for Small Businesses, then the proactive management of cyber-risk across the DIB can be achieved.

Small Business leaders need to think differently about how they operate within an actively contested cyber environment to create impactful and sustainable change. Leaders must proactively manage their third-party providers, implement effective contract(s) management, oversight and delineate roles and responsibilities concerning cyber controls, incident response and reporting. Small Businesses need to adopt new knowledge and skills to understand how to scope and manage the cyber-risk to their operations, and implement effective strategies to manage the risk. As cyber

regulation develops Small Business owners will need to ensure cyber-risks are effectively mitigated, if they wish to be considered for Federal and commercial contracts.

An appropriate way forward is to enable Small Business to baseline their cyber compliance, using CPAs as their trusted advisors to assess their current cyber compliance against an agreed baseline. Together, Small Business and CPAs can put in place an appropriate plan of action to mitigate cyber-risks and manage appropriate controls, enabling Small Business to transfer their critical IP to cloud providers along with appropriate controls. Transferring appropriate data and cyber controls to the cloud will support the chain of custody of the Small Business IP and will increase data security, efficiency, effectiveness and reduce the cost of cybersecurity compliance. Ahead of companies developing and implementing their own cybersecurity strategy.

The Augusta Plan

About the authors

Andy Watkin-Child is a 20-year veteran of cybersecurity, risk management and technology. He has held international leadership positions in 1st and 2nd Lines of Defence (LoD) for cybersecurity, cyber-risk management, operational risk, and technology. For companies across Engineering and Manufacturing, Financial Services and Publishing and Media. Working with leadership teams of companies with balance sheets over €1TRN. He is an experienced member of management boards, global risk leadership teams, cybersecurity, operational risk and GDPR committees.

Andy holds Royal Charters in Security (CSyP), recognised by the UK Centre for the Protection of National Infrastructure (CPNI) and Engineering (CEng). He has a place on the UKs Register of Chartered Security Professionals. He is a member of the Board of the Security Institute (MSyI), the largest UK members only security trade association, he is a Freeman of the Worshipful Company of Security Professionals (WCoSP) and a Freeman of the City of London. He is a counsel appointed expert witness who specialises in cyber and risk management a Practicing Associate of the Academy of Experts (AMAE) and advised the Information Commissionaires Office (ICO) on high profile GDPR cases. He is a member of the U.S. CMMC Accreditation Body (CMMC-AB) standards working group, developing the CMMC assessment methodology. Chair of the UK Team Defence Information (UK-MoD) CMMC Working group. Working with UK defence trade associations in support of the deployment of CMMC into the UK DIB.

Andy is the Founding Partner of Parava Security Solutions an independent Cyber-risk Management advisory firm, supporting organizations deliver cyber-risk management and cyber regulatory programmes. He runs CMMC Europe, an advisory company focusing on supporting the European DIB deploy CMMC www.cmmc-eu.org

https://www.linkedin.com/in/andywatkinchild/

Ted Dziekanowski is a veteran of cybersecurity with over 40 years' experience of the design, delivery, oversight and assurance of cybersecurity and risk management systems. Ted's area of expertise is the management of risk in Information Technology developed over the years. He is an experienced systems Auditor and Integrator giving him a unique insight as to the challenges associated with developing an eGRC program that satisfies the compliance requirements faced by organizations of all types and sizes.

He is an internationally recognised cybersecurity, risk management and Information system auditor. A highly respected security trainer, authorized to train ISACA CISA, CISM, CRISC, ISC2 CAP, CCSP, and CISSP. He holds DoD secret clearance and has taught causes for a broad range of public and private sector (available on request)

https://www.linkedin.com/in/tdziekanowski/

Jason Spezzano is an experienced cybersecurity services delivery leader and consultant with over 25 years of experiences. Specialties include risk management, compliance, and cybersecurity operations supporting DoD, Federal and Intelligence Agencies. Jason is currently the Senior Director of Cybersecurity at Grammatech, a leading developer of software-assurance tools and advanced cybersecurity solutions, as well as a Senior cybersecurity consultant focused on Governance, Risk Management and Compliance (GRC) using information security frameworks established by the National Institute of Standards and Technology (NIST).

Jason is also a Fellow with the Cybersecurity Forum Initiative (CSFI) and a former Major in the United States Marine Corps.
https://www.linkedin.com/in/jason-spezzano-aaa862b/

Brian McCarthy is the founder and President of 327 Solutions, Inc. Since the early 1990's Brian has been in training design and delivery, having gained experience in the Pharmaceutical and Biotech, Manufacturing, Defense, Finance, Legal, and additional business verticals. With experience creating programs that enable competency and certification outcomes through traditional workshops and strategically blended learning systems delivering messaging over time, 327 maximizes competency transfer to the job. 327 focuses on the right solution to get everyone to their goal.

- He has experience at Sybex Publishing working on ISC2 Official Study Guides as a technical editor.
- Brian and his team deliver the highest calibre trainers globally, many of whom are contracted directly by leading non-profit and educational organizations such as ISACA, ISC2, EC-Council and others.
- Brian is a former trainer (Windows NT/2000), and sees training delivery through the eyes of a trainer, focused on quality and student outcomes.
- He has deep expertise in the development of blended learning system leveraging pre-work, intensive workshops, eLearning development, gamification, mobility of learning assets, and continuance of learning.

https://www.linkedin.com/in/bmccarthy/

Reference

1. US GDP: https://advocacy.sba.gov/2019/01/30/small-businesses-generate-44-percent-of-u-s-economic-activity/
2. Small Business Administration (Office of Advocacy): https://asq.org/quality-resources/small-https://cdn.advocacy.sba.gov/wp-content/uploads/2019/04/23142719/2019-Small-Business-Profiles-US.pdf
3. American Society of Quality (ASQ):https://asq.org/quality-resources/small-business#:~:text=Small%20business%20is%20defined%20as,corporation%20or%20regular%2Dsized%20business.&text=The%20U.S.%20Small%20Business%20Administration,standards%20based%20on%20specific%20industries
4. National Association of manufacturers: https://www.nam.org/facts-about-manufacturing/
5. US Bureau of Economic Analysis: https://www.bea.gov/
6. US DOD Office of Small Business: https://www.defense.gov/News/News-Stories/Article/Article/2416891/small-businesses-key-to-nations-defense/
7. F-35 Aircraft Sustainment, DoD Needs to Address Substantial Supply Chain Challenges: https://www.gao.gov/assets/700/698733.pdf
8. Government Accountability office (2018): Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities
9. Government Accountability office (2018): Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation
10. Government Accountability office (2021): WEAPON SYSTEMS CYBERSECURITY Guidance Would Help DOD Programs Better Communicate Requirements to Contractors
11. Government Accountability office (2021): Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight
12. Office of the Inspector general US DoD (2019): Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems DODIG-2019-105
13. Government Accountability office (2020): 2020 Defense Acquisition Assessment
14. Deloitte, Wall Street Journal IT spend as a percentage of revenue. https://deloitte.wsj.com/cio/2018/03/12/it-spending-from-value-preservation-to-value-creation/
15. Deloitte. Reshaping the cybersecurity Landscape: Financial Services cyber spend
16. Forbes: Banking spend on technology
17. JPM Morgan: Cybersecurity Spend
18. Banks suffer more cyber-attacks: https://www.ciodive.com/news/cyberattacks-hit-financial-services-300-times-more-than-other-sectors/557372/
19. NIST SP 800-171A Assessment: https://csrc.nist.gov/publications/detail/sp/800-171a/final
20. AICPA SoC 2 reports: https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/serviceorganization-smanagement.html
21. AWS SoC report: https://aws.amazon.com/compliance/soc-faqs/
22. The cost of a cyber-attack: https://www.insurancebusinessmag.com/us/news/cyber/global-cyber-insurance-pricing-spikes-32--report-259795.aspx