Cybersecurity is a Constant Challenge

43%

of small businesses were victims of breaches in 2019[1]

350,000

new malicious programs are detected everyday[2]

24%

of breaches were due to human error[3]

Are you prepared?

With a constantly evolving threat landscape, it is hard to know if you are doing enough to mitigate the security risks to your business, your data, and your people. At Risk Alleviators Technologies, it is our mission to help small and medium sized organizations make informed security decisions when it comes to their specific risk profile. With over 15 years of commercial and high-security government entity experience, Eric Chapman, Senior Consultant at Risk Alleviators Technologies, can advise and help implement security improvements across your infrastructure and software, develop employee policies and conduct training.

RISK ALLEVIATORS
TECHNOLOGIES

Trusted advisors for customized security services

www.RiskAlleviatorsTech.com

SERVICES

> *“The combined effect of the IR (Incident Response) team and IR plan testing produced a greater cost savings ($800,000 to respond to a breach) than any single security process.”[3]*

> *“While malicious breaches were most common, inadvertent breaches from human error and system glitches were still the root cause for nearly half of the data breaches...”[3]*

> *“58% of companies found over 1,000 stale user accounts.”[4]*

> *“1 in 2 companies are unable to cope with remote work security risks”[5]*

CONSULTATION SERVICES

Securing your organization is a balancing act between reducing risks and budget. Most organization leaders need help to determine the right-level of security investments. We have the experience of framing an organization’s security risks in terms and actions that enable senior leaders to feel confident in their security posture.

Business Risk Management – assess the organizations security risks, current practices, policies, and compliance requirements to develop a set of prioritized recommendations. We then consult with management regarding actions and budget trade-offs based on prioritization of risks.

Disaster Recovery and Business Continuity Planning – document a robust set of operating procedures for use in the event of a disruptive event, security threat or breach. Test the plan and train the organization on procedures to put the plan in motion.

Internal Threat – perform an in-depth assessment to evaluate both malicious and inadvertent threats from employees.

CYBERSECURITY ASSESSMENTS

Often internal systems are misconfigured or not kept up to date creating an opening for miscreants. Our advisors can assess a wide range of infrastructure, policies, and practices on a one-time, quarterly, or annual basis.

Access Control – auditing of physical and virtual access technologies and restrictions to ensure only authorized personnel are allowed access.

Vulnerability Assessments – evaluation of the organization’s vulnerability management systems and processes including vulnerability scanning, analysis, penetration testing, and reporting. Assessments can be conducted as part of review or for a breach forensics investigation. Our advisors have in-depth experience with various security scanning tools within open or closed networks.

Malware/Virus Protection – assessment of the organization’s current malware protection solution to evaluate efficacy against the latest threats. We can also independently investigate replacing your malware protection solution and recommend the best fit for your organization.

Telework Security – assessment of telework services and methods to ensure telework and virtual conferencing methods are properly secured to prevent leakage of sensitive data.

COMPLIANCE ASSESSMENTS

Failing an audit can highlight preventable risks and be a significant cost to your organization. With our experience in highly regulated organizations, we can prepare you to sail through your next audit.

> *“Sizable fines assessed for data breaches in 2019 suggest that regulators are getting more serious about organizations that don’t properly protect consumer data.”*[6]

Security Control Assessments – assessment based upon the Center of Internet Security (CIS) Critical Security Controls, National Institute of Standards and Technology’s (NIST) Risk Management Framework (RMF) or NIST Cybersecurity Framework to assess the measures to protect your critical assets.

Compliance Audits – review organizational policies, procedures, guidelines, and technology controls to ensure compliance with industry standards. Applicable frameworks include: Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act, Federal Information Security Management Act (FISMA), Payment Card Industry Data Security Standards (PCI-DSS), and for organizations doing business in California: California Consumer Privacy Act (CCPA), or Europe: General Data Protection Regulation (GDPR).

SECURITY HARDENING SERVICES

You need to first define which assets, data, systems, and hardware are the most vital to your organization with an assessment. Once that is complete, a policy around these items can be built and implemented to properly secure and safeguard them. In our experience, our consulting has led to better system engineering and performance while maintaining system availability. Security hardening can be commissioned on a one-time, quarterly, or annual basis.

> *“Misconfigurations are a common cybersecurity gap. Security experts agree that configuration errors in privileges, endpoint settings, internet settings, risky services needlessly enabled, and bad access control configurations are leading causes of cybersecurity incidents especially in small and medium business environments”*[7]

Data Security - consultation on how to protect data at-rest or in-transit. Consultation includes database security (SQL Server, Oracle).

Application Security – consultation on security hardening on an application, server, network, or infrastructure level.

Operating System Security – consultation on measures to protect Operating Systems (OS) from threats across infrastructure such as personal computers, switches, firewalls, IoT devices and more. This may include patching, updating anti-virus software, configuring a firewall, and advising on access controls.

> *“8 in 10 companies have experienced a data breach made possible by cloud misconfigurations”*[8]

Network Security – security hardening recommendations for firewalls, Virtual Private Networks (VPNs), Cross Domain Solutions (CDS), cloud and more.

TRAINING

Effective training can reduce many factors that enable security breaches. We can conduct training for your technical staff, or your general employee population based on the top risks to your organization.

> *“Human error as a root cause of a breach includes “inadvertent insiders” who may be compromised by phishing attacks or have their devices infected or lost/stolen. These were responsible for about one-quarter of breaches.”*[3]

Security Awareness – Ponemon Institute found that employing employee training is in the top 6 recommendations that reduce the potential cost of a data breach[3]. Training topics can be focused on themes such as recognizing phishing or protecting yourself and your company while working remotely.

Security Hardening - We can train your staff on security hardening practices on your systems. Our training will provide personnel with the confidence that they can strengthen the technical security measures of their systems at various levels of their infrastructure.

3 Reasons to Choose Risk Alleviators Technologies:

Agility

We have vast experience across many aspects of an organization's security requirements. This enables us to serve as a single, vendor agnostic resource to advise small and medium-sized businesses and government organizations. We can help both the technical teams and senior management with customized recommendations to alleviate risks. We are dedicated to being responsive, transparent, and supportive in the on-going challenges to maintain your security protections.

Experience

With extensive experience in high security U.S. government organizations, we have the depth of expertise and rigor to consult on a wide range of security areas including Risk Management, Vulnerability Management, Security Compliance, Security Assessment, Auditing, Security information and event management (SIEM), Data Security, and Security Engineering. We can also support the implementation of strategies from security hardening systems to training.

Affordable

Our agility enables us to customize our services to your organization's needs. You pay for only the services you most need based on your specific situation including risks and compliance requirements.

EXPERIENCE

Eric Chapman is the Founder and Senior Consultant at Risk Alleviators Technologies. Eric is an accomplished security expert with 15 years of diverse working experience in the Information Technology and Security industry for high-security U.S. government entities. Eric is known for his ability to work effectively across organizations from the IT technical teams to senior leadership. Eric brings extensive experience in executive reporting, compliance, information assurance, risk management, information security, vulnerability management, and technical support.

Certifications

- Certified Information System Security Professional (CISSP)
- EC-Council Certified Security Analyst (ECSA)
- EC-Council Certified Ethical Hacker (C|EH)
- Security +
- Amazon Web Services (AWS) Certified Cloud Practitioner

Also, DoD 8570/DoDD 8140 Compliant: IAT Level III, IAM Level III, and IASAE Level II

CERTIFICATIONS AND PROFESSIONAL ASSOCIATIONS

MBE, DBE, SBE CERTIFIED

Maryland Department of Transportation (2019)

Cybersecurity Association of Maryland (CAMI)

Prince Georges County Chamber of Commerce

Greater Bowie Chamber of Commerce

U.S. Black Chambers, Inc.

NAISC CODES

- 541512 – Computer System Design Services
- 541513 – Computer Facilities Management Services
- 541519 – Other Computer Related Services
- 541611 – Administrative Management and General Management Consulting Services
- 541690 - Other Scientific and Technical Consulting Services
- 611420 – Computer Training
- 611430 – Professional and Management Development Training

All organizations are at risk of a cyberattack, no matter their size. The key to protecting your organization is proactively designing a robust risk mitigation plan as well as a strong incident response plan should your organization become a victim of a security breach this year. Get the help you need to proactively plan your security defenses.

Contact us today at hello@riskalleviatorstech.com

RISK ALLEVIATORS TECHNOLOGIES

www.RiskAlleviatorsTech.com

1 Verizon, 2019 Data Breach Investigation Report
2 AV-Test Institute GMBH, July 2020, Malware Statistics
3 Ponemon Institute, 2019, Cost of a Data Breach Report sponsored by IBM Security
4 Varonis, 2019 Global Data Risk Report From the Varonis Data Lab
5 Filip Truta, July 2020, One in 2 Companies Unable to Cope with Remote Work Security Risks
6 Dan Swinhoe, Editor, CSO, January 2020, The Biggest Data Breach Fines, Penalties, and Settlements so far
7 Filip Truta, June 2020, Top 5 Endpoint Misconfigurations That Open Security Gaps [Whitepaper]
8 IDC Survey, June 2020, Ermetic Reports Nearly 80% Experienced a Cloud Data Breach in Past 18 Months