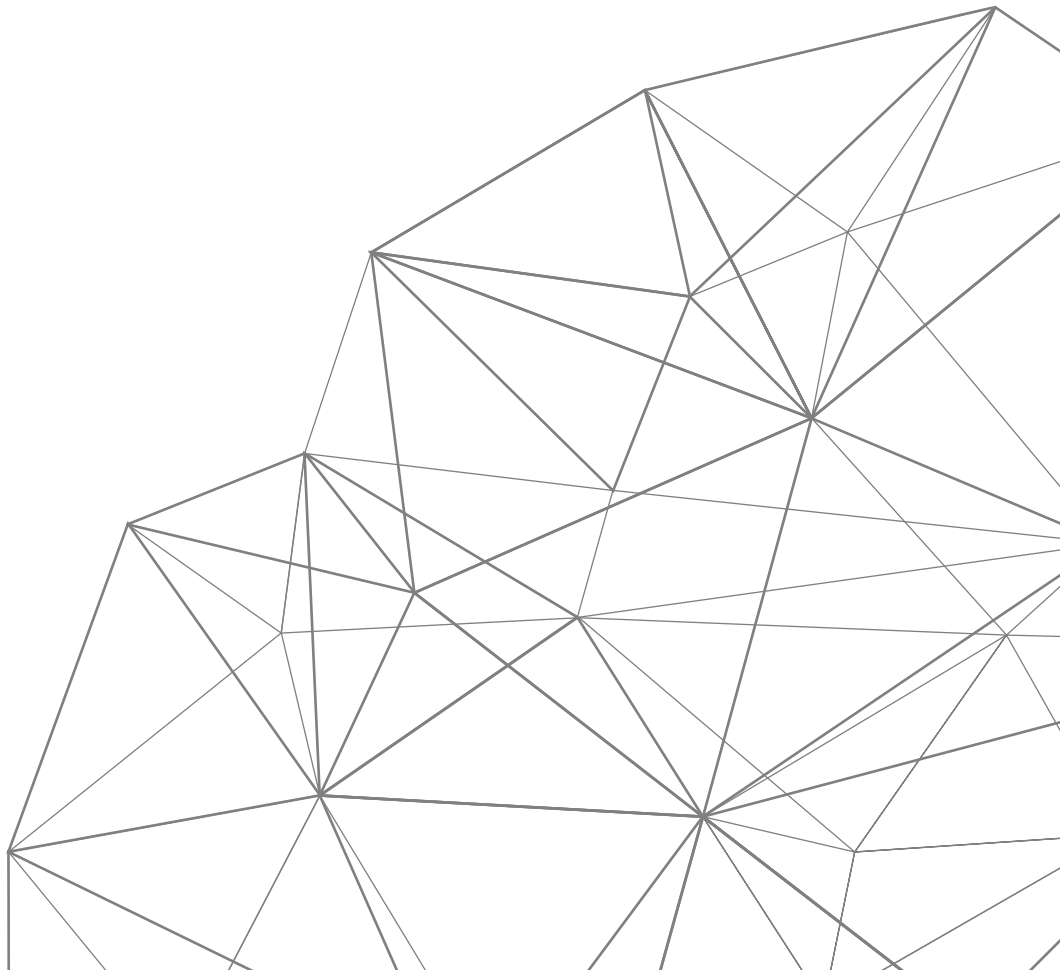





SECURITY TRAINING 101

Whitepaper



A large, white, stylized number '1' is positioned on the left side of the page, set against a dark green background with small white dots.

We work with clients big and small across a range of sectors and we utilize our resources to ensure that your problems are handled with care. We believe that analysis of your company and its systems is key in responding effectively to your systematic needs and we will work with you to fully understand your business tech needs to achieve the greatest amount of success as possible so that you can see a true value from your tech investment.

We have a number of different teams within our agency that specialize in different areas of business so you can be sure that you won't receive a generic service and although we can't boast years and years of service we can ensure you that is a good thing in this industry. Our teams are up to date with the latest technologies, media trends and are keen to prove themselves in this industry and that's what you want from a technology agency, not someone who is relying on the same way of doing things that worked 10 years, 5 years or even a year ago.

Whatever the level of support you require, we are sure that we will have a package that meets your needs. All of our virtual professionals are highly experienced in the areas in which they work and have been through a thorough recruitment process to ensure they deliver to the high standard that you would want for your business.

We will work with you to fully understand your business and your technology needs and digital strategy. Using the outcomes from the Technology Analysis, we will put together a plan for the most effective technology strategy to get the best results for your business

1 INTRODUCTION

Security awareness training is one of the most critical and important security requirements for any size organization to consider implementing within their environment. Arguably, the greatest risk faced by any organization is the danger of insider threat as employees are can be considered a weak link in the chain as they are susceptible to curiosity, greed, envy, etc. To further increase risk, employees may be faced with the threat of social engineering attacks including phishing, baiting, spear phishing, tailgating, scareware, pretexting, quid pro quo, etc. To combat these risks, a strong security awareness training program can be leveraged to properly inform employees of the security risks they may be presented within the workplace and how to properly observe, defend, and report any suspected malicious activity.

What is social engineering and am I affected?

Simply speaking, there is more to cybersecurity than computers and how they work. This statement includes how your network is setup or even how your firewall is configured, etc. Within cybersecurity there is actually a heavy emphasis on people as they interact directly with data within the organization. These people (employees) can have duties such as maintaining computers, configuring computers, helping others with computer problems, etc. and tend to not be as rational as computers as they can be swayed by emotion. This human factor is what social engineering attacks attempt to exploit to achieve whatever malicious goal may be present. In many serious cases, this can result in an attacker gaining access to systems that they would not normally be authorized.



This human factor is what social engineering attacks attempt to exploit to achieve whatever malicious goal may be present.

Have you ever received phone calls from telemarketers that sounded like a scam? Have you ever received emails posing to be from legitimate organizations requesting abnormal information? Have you ever received random text messages requesting you to follow unidentifiable links? If so, you have most likely been a potential victim of sort of a social engineering attack.

Just as common practice as these attacks are on us individuals, they can be even more common and damaging to an organization. Social engineering attacks are not something new; however, they have recently become so common that most of us have seen or been affected by an attack in our lifetime.

What services are offered?

Here at Grove Technologies, we offer a security training program in a three-tiered approach which includes services such as a staff training portal, staff training videos, dark web scans, anti-phishing training, auto-phish email testing, staff security certifications, business impact analysis, and business continuity planning. Depending on the need of the organization, there is a plan that will fit your requirements.

More specifically, one feature of our services includes a staff training portal with a user-friendly dashboard for easy navigation. This portal allows for successful management, metrics, and tracking to assist with confirming all required training activities are completed within the organization. Employees that successfully complete the desired training will also receive security certificates for additional tracking and validation as needed.



Employee Awareness

Monthly security newsletter and personal dark web scanning capabilities allow employees to protect themselves at work and at home.



Documentation Tracking

With written security policy templates and a policy acknowledgement portal, ensure your employees know the proper procedures while tracking your annual agreements.



Dark Web Protection

Ongoing dark web monitoring alerts you the moment employee credentials show up on the dark web. Push password resets and stop a breach before it happens.



Fortify Human Defenses

92% of data breaches are caused by human error. Annual security training covers the basics while ongoing weekly micro-security training keeps users up-to-date.



EVA Brings It All Together

EVA, our Employee Vulnerability Assessment, takes these key security metrics and adds engagement with an interactive leaderboard and friendly competition!



Email Phishing Protection

Phishing is the #1 attack method of choice among cybercriminals. AutoPhish keeps security top-of-mind with automated, simulated phishing campaigns.

**Providing cutting
edge cybersecurity
training for small
businesses since
2014.**



WHAT ARE THE BENEFITS?

A good security awareness program teaches

employees the information they need to protect themselves and their organization's assets from loss or harm. Grove security training services accomplishes this mission by ensuring the human risk factor is mitigated by supplying employees with the information and knowledge on the threats they may be faced with in the workplace. Employees may be considered one of the weakest links; however, they are also known many times as the first line of defense. Below are some of the key benefits to utilizing Grove security training services

Grove Training Services	
Ensure compliance with applicable regulations	Prevent security breaches
Protect your customer and/or client data	Peace of mind
Change culture (personal use, phones, social media, etc.)	Cost effective vs a data breach

Is security training a requirement?

A major factor for an organization to have a strong security training program is to achieve a level cybersecurity compliance that is required by a customer or a specific contract. As an example, security training is required for all organizations who have contracts with the Department of Defense to comply with the DFARS and NIST SP 800-171 requirements. In more recently emerging news, the Department of Defense announced the creation of the Cybersecurity Maturity Model Certification (CMMC). This certification will validate that a contractor has not only met the applicable security controls from NIST-171, but also adds three additional frameworks. The CMMC process will require contractors to be assessed by a pre-approved outside audit company to ensure they have met all required and applicable DOD security standards before allowing them to win future federal contracts.

Even if your organization is not required by any specific compliance requirements or certifications, the value still resides with the protection of your organizations data and assets. Security training will assist with the first line of defense (employees) are properly informed and have the knowledge of how to properly act during a potential threat scenario.

2

COST

Cybersecurity Training should not cost an arm and a leg. Get high quality, automated, cybersecurity training at a fraction of the cost from Grove Technologies.

HOW MUCH WILL IT COST?

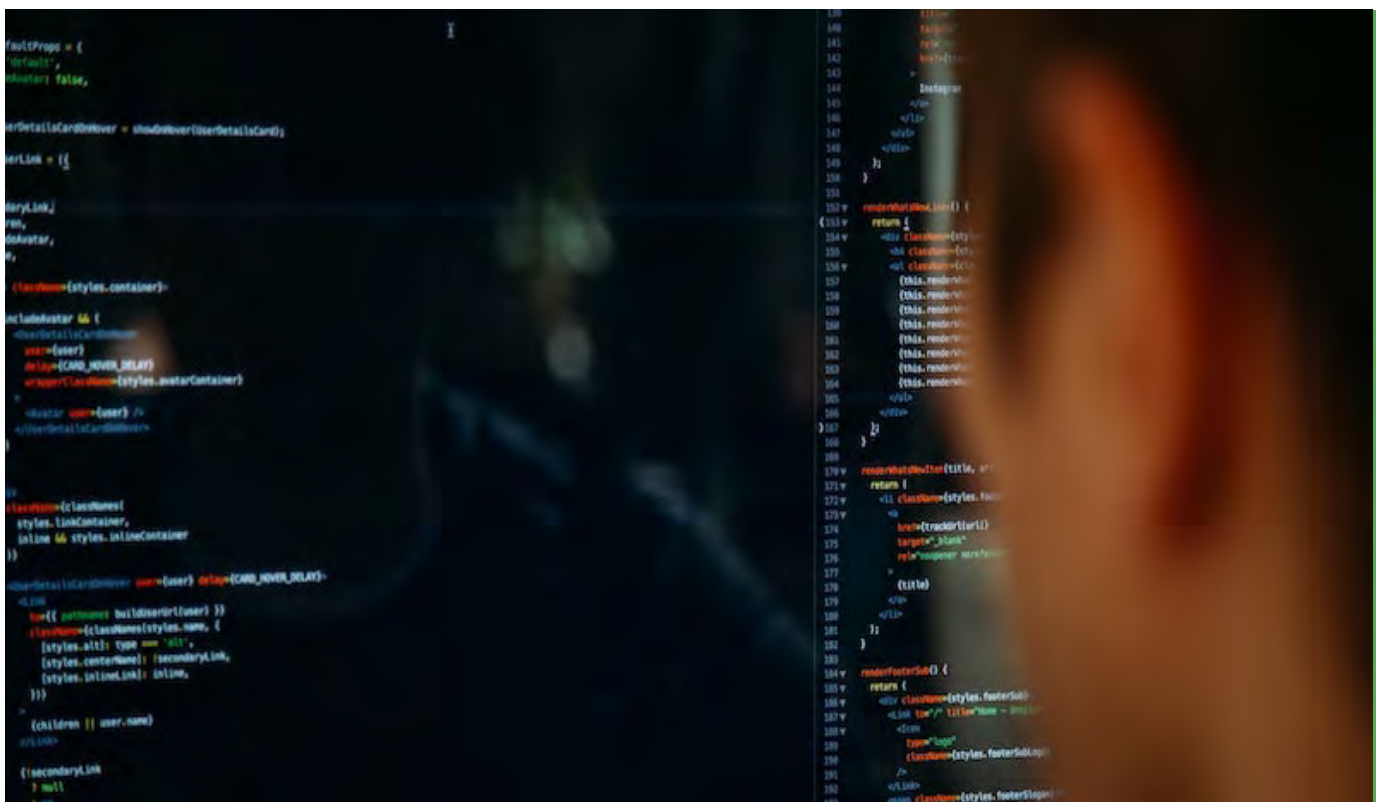
Best Value

The cost of obtaining security training services will depend on the size and needs of the organization. Here at Grove Technologies, we offer a three tiered approach including a starter package (start-ups), a business package (small businesses), and an enterprise package (large companies). Each one of these services are designed with the customer in mind to ensure an affordable approach to the appropriate level of service needed to meet any security compliance requirements that may be present.

How Do I Get Started?

Still have additional questions about security training? Schedule an appointment with us today! At Grove, we have the expertise and knowledge to support you with a wide range of various information security concerns and compliance requirements.

CALL US TODAY!
(888) 253-9103



Dark Web Monitoring

Proactively monitor the dark web for compromised account data. The sooner end-users are notified of a breach, the sooner they can change their passwords. End-users also have the ability to scan the dark web for their personal, friends, and family accounts with no limit.

AutoPhish

Routine simulated phishing has been proven to minimize the risk of end-users falling victim to a malicious phishing attempt. Routine phishing instills into our users the very behaviors of IT professionals before they click on any link so that even on the most chaotic of days, they're ready.

Continuous Education

Weekly 2-minute micro-training video & short quiz combined with a monthly security newsletter keep cybersecurity short, engaging, and interactive. White-labeled emails sent on your behalf to all your users means hands-off management

Written Security Policies

Security policies are key to establishing expectations and explaining repercussions to protect your client organizations. Our document management portal contains a variety of customizable security policies from BYOD to Security Incident Response.

Interactive Leaderboard

For end-users, an interactive leaderboard ignites friendly competition with just their screen name's honor at stake. For managers, employee names are featured, with a report for performance evaluations, they can track just who needs more time bulking up!

Security Risk Assessment

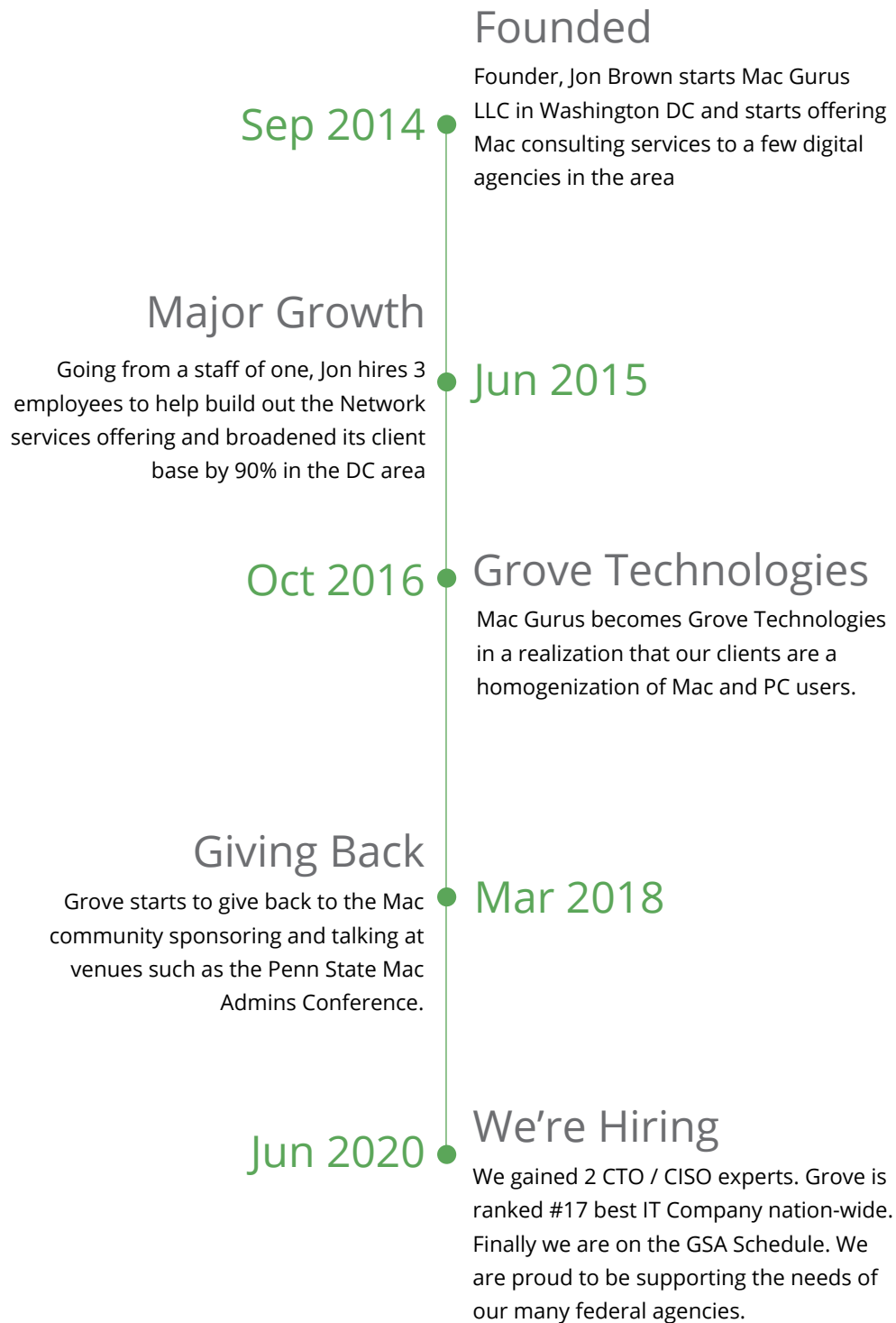
EVA identifies the human vulnerabilities and their related risks. Based on NIST standards, our Security Risk Assessment (SRA) assesses your client's administrative, physical, and technical vulnerabilities; identifies the associated risks, and provides recommendations for improvement.

Best Cybersecurity Consulting, for Your Business.

Your business is only as good as the people that work there. Its time to train your employees the right way with our security awareness program. With next generation analysis of key security metrics to rank your employees by their associated risk level with our Employee Vulnerability Assessment.



ABOUT GROVE TECHNOLOGIES



MEET THE TEAM



Jon Brown

CEO & FOUNDER

Jon is a charismatic leader, entrepreneur, teacher & mentor who helps businesses take their Mac, Cybersecurity & Networks to the next level.



Scott Campbell

CISSP & VCISO

20 years of experience in providing executive consulting for cybersecurity and IT clients needs in a vCISO role for compliance, CMMC and more.



Michael Tedesco

CISSP & VCISO

With a background in the US Coast Guard, Michael helps the needs of our Government companies stay within the boundaries of compliance.

Contacts Us

Adress

1030 15th St NW Suite 1050w,

Washington, DC 20005

Phone

(888) 253-9103

(240) 451-8688

Email

support@grovetech.co



Consultants Network