CyberSecurity

VESTIGE
Digital Investigations

Overview of Services

Experience, Preparation & Quick Response are Key

In today's 'always on' society, organizations are digitally connected to their employees, customers, suppliers and other stakeholders. As a result, the opportunities of experiencing a CyberSecurity incident are significant. There is a clear correlation between lower costs, improved customer retention and maintaining reputation for those organizations that are ready and best able to prevent, detect and respond to CyberSecurity issues.

At Vestige we also recognize Information Technology work expectations are at an all-time high and IT departments are often pulled in too many directions to address some of the proactive and reactive security and forensic work in a timely fashion. We can help.

When an organization faces a CyberSecurity threat, time is of the essence for identifying the malicious activity, how the incident occurred, removing the incident and taking all the required follow-up actions. Getting the organization back to normal operation is always the primary concern — but far too often additional security measures and preservation of evidence can get overlooked in the rush to return to normal operation.

Organizations benefit from Vestige's CyberSecurity and Digital Forensic expertise because we evaluate the *Actual Threat Environment™* - the entire scope of risk, including:

- **Identifying the cause** and assess the scope of an incident
- **Preserving the evidence** to support any notification duties and potential litigation
- **Understanding the totality of the situation** to ensure remediation is complete and assist legal with any Notification Obligation determination
- **Recommending an appropriate course of action** to prevent/follow-on or mitigate future attacks.

Vestige Digital Investigations offers trusted and extensive CyberSecurity experience to organizations. While we all realize no organization can protect themselves 100 percent, our clients engage us to identify, prioritize, strategize and minimize their surface of attack and to put the necessary controls in place to prevent/follow-on and respond to CyberSecurity incidents through the following offerings:

Proactive Services - planned, actionable expert solutions to prevent incidents

Reactive Services - swift, leading edge response to significantly mitigate damage

Cybercrime **Costs**

- US Cybercrime costs are up 23%
- $7.9 Million = average cost of Cybercrime to organizations
- US Military now treats it as one of their five domains: Air , Sea, Land, Space and Cyber
- 80% of U.S. businesses expect a Critical Breach
- 1 in 3 companies are not prepared

Data Breach **Stats**

Global Study At A Glance - 477 companies:

- $3.86 Million is the average total cost of data breach
- 6.4% increase in total cost of data breach over 2017
- $148 is the average cost per lost or stolen record
- Save $14 per record with an Incident Response Team

— Ponemon Institute Research Report, May 2018

Proactive Services

Preventive Actions to Stop Incidents & Data Breaches Before They Occur

Assessments

Vestige offers a wide variety of assessments to find and remedy or add new environmental Controls.
Types of assessments include: **CyberSecurity Readiness, Vulnerability Scanning, External Penetration Testing**, and **Compliance Audits**. For proactive data security, it is best to have your current environment comprehensively assessed.

BreachReady™

It's easier to solve a problem when you already have a contract in place and a service on speed-dial. Vestige's BreachReady™ is a retainer agreement that allows organizations to do just that. With BreachReady™ Vestige learns about the environment up-front and regularly monitors to validate it. So if or when there is a breach, the organization does not waste valuable time vetting out an effective service. Vestige is contracted and ready to jump right in to solve any data breach issue that arises.

CyberSecurity Awareness Training

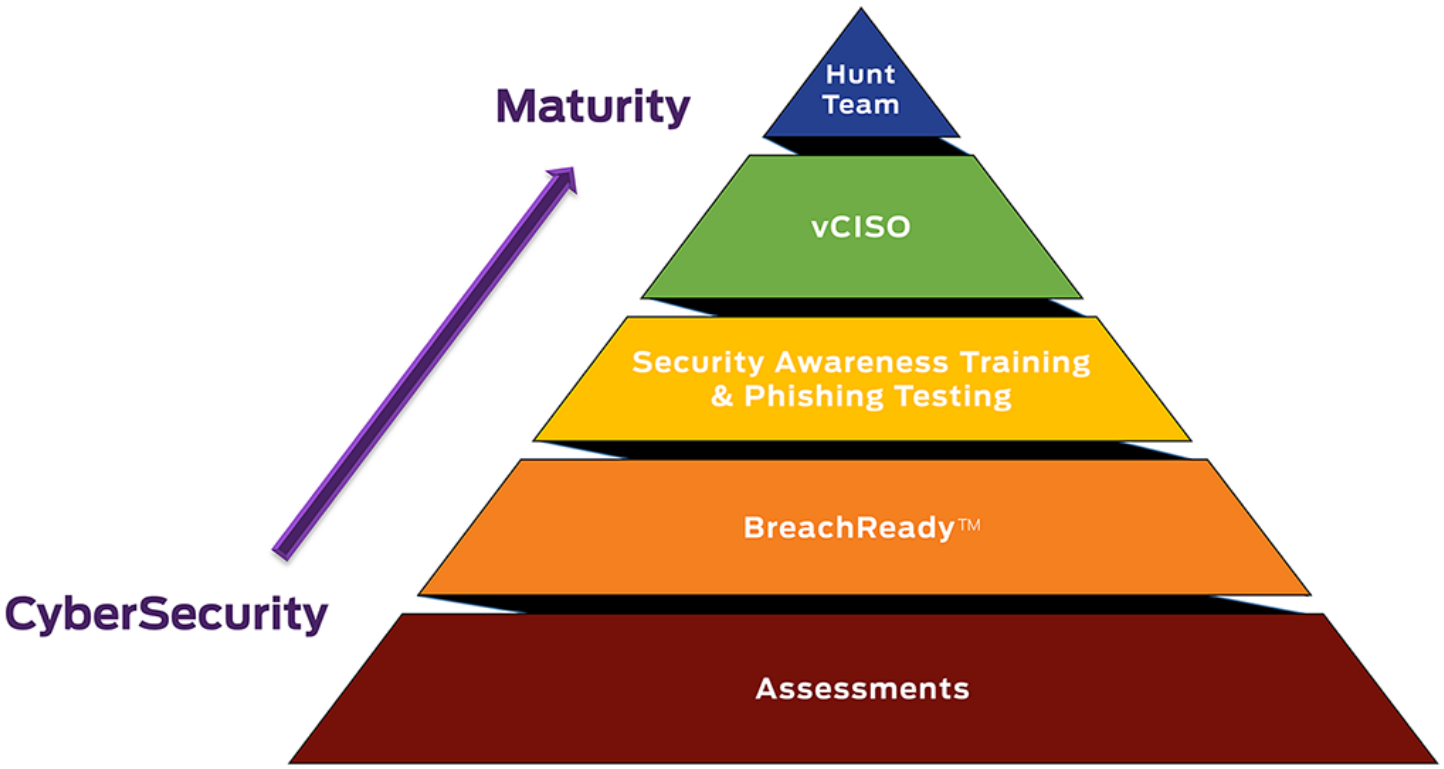
It is well established that the majority of today's CyberSecurity incidents are caused, directly or indirectly, by the end-users. Until your users can recognize and learn to spot the tactics that attackers are using – your company IS at risk of a cyber compromise or breach. Through our CyberSecurity Awareness Training, Vestige combines a variety of educational tools to ensure that users fully understand safe CyberSecurity practices on a continuing basis. Live training, quizzes, recorded webinars, phishing expeditions and visual collateral are all a component of this service which can be easily customized for your organization.

Virtual CISO

At Vestige we understand there is no "one size fits all" in the business world. Information Security needs, big and small, simple and complex, are unique to every company and industry. Because there's no one model for success, businesses require customized solutions. Vestige's Virtual CISO offers a flexible and affordable alternative for organizations that need access to high-level Information Security expertise but don't want to hire a full-time Chief Information Security Officer (CISO). Many companies do not have a full-time Chief Information Security Officer, however they require the duties this position offers. With Vestige's Virtual CISO , Vestige functions as your organization's CISO remotely.

Hunt Team

Vestige's team of cyber investigators continuously search through the network to look for active indicators of pre-breach attempts. They identify the markers and red flags that attackers leave behind as they are performing their reconnaissance. Vestige looks for privilege escalation, persistence and the myriad steps they take in attempting to "own" your secure data. The Vestige Hunt Team then stops or greatly mitigates the attack BEFORE it can occur. Choose Vestige for this long-term agreement to assist your IT security team with counterintelligence in a flexible and fiscally responsible way.



The CyberSecurity Maturity Process

GAINING CLARITY

The first step organizations take when beginning a Proactive CyberSecurity process is to have a comprehensive I.T. **Assessment**. This is broad and comprehensive look at the entire environment that allows Experts the opportunity to find all the gaps in the current system. Yes, the organization may have a firewall and meet specific industry compliancy standards, however, many gaps typically exist outside of these. The assessment gives you a starting point as to what areas are secure and what areas are a perfect entry way for hackers and need work.

PREPARING

After the Assessment many companies opt to have a contracted service in place should an Incident or Breach occur. That's why they implement the **BreachReady™** service.

Wise organizations then implement a staff **Security Awareness Training** program to regularly bring CyberSecurity to the front of mind. This includes testing staff with anonymous awareness tests for Phishing -- as human error is often a root cause of breaches.

REMAINING VIGILANT

As the overall knowlege of the organization matures in regards to CyberSecurity, the next steps include a Virtual Chief Information Security Officer or **vCISO** for on-going, high level expertise of compliance, education and program roll-outs.

Finally, mature organizations then elevate to the sophisticated **Hunt Team** service. A necessary augmentation to traditional security practices. The Vestige Hunt Team focuses on the incident response space complementing traditional passive monitoring detection efforts with a proactive means to identify, mitigate and remdiate threats on an on-going basis, before a breach occurs.

CyberSecurity

Reactive Services

Vestige is Your Urgent Response Experts

Incident Response | Data Breach

Vestige offers leading edge experience at being parachuted in to quickly assess, stop and remedy the damage for an incident or data breach.

Malware Analysis

Vestige is able to reverse engineer malware to determine the payload impact on your IT environment.

Root Cause Analysis

Our Root Cause Analysis Service utilizes Vestige's proven approach, tools and techniques to systematically process your data breach and accurately identify the cause of the incident.

Ctrl-Alt-Del IT Reboot

Organizations should never feel captive by their IT Department. This service provides a solution for quiet and effective transitional control of your digital environment should IT staff in critical positions leave unexpectedly, pass away or are being let go. Vestige will step in and provide a timely, smooth temporary take-over of the IT environment and transition to replacement personnel -- all with minimal disruption to your organization.

Contact Vestige today for CyberSecurity Services.

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com