CyberSecurity

VESTIGE Digital Investigations

Actual Threat Environment™

Proactive CyberSecurity Assessment Readiness

You need only read daily news stories to understand the challenges and threats that data breaches now pose for business. Once a breach occurs, millions of dollars can easily be lost to fines, penalties, attorney fees, remediation expenses, lost customers and harm to reputation, trust and confidence. It's not just a problem for certain types or sizes of business — today, all industries and all organizational sizes are being affected.

Companies spend significant money on IT solutions establishing a layered set of Internal Controls to manage threats of the business' vulnerability or 'Actual Threat Environment' (ATE) is broader than these Internal Controls. Unfortunately, because the threat environment is so dynamic, a significant 'gap' between Actual Threat Environment and Internal Controls has become the norm for business.

An organization's *Actual Threat Environment™* reflects the entire scope of risk and its complexity: business strategies, underlying electronic devices, network configurations, security, policies, persons, companies, relationships, case law, and regulatory environment within which the organization operates.

Together all of these components comprise a modern business/legal/technical/social environment and need to be considered when evaluating risks to an organization's Actual Risk Environment.

Key **Points**

- Understand your organization's *Actual Threat Environment™*
- Go beyond compliance
- Prepare for tomorrow's unknown risks today

An Actual Threat Environment™ May Include:

- Exposures inherent to using multiple technologies and electronic devices
- Unsecure third party applications resident on mobile devices
- Use of personal devices in the workplace such as cell phones
- Use of mobile monitoring devices within medical and other industries
- Virtual work environments and other changing work behaviors and attitudes
- Criminal and politically sanctioned data threats
- Limitations of regulatory based audits and internal controls to only specific data types
- Expanding regulatory enforcement and expansion of the definition of protected data
- Evolving third party business relationships and trusted communications channels
- Limitations of indemnification provisions within vendor agreements
- Expanding case law decisions, especially in the area of privacy without regard to data type
- International business behaviors and policy

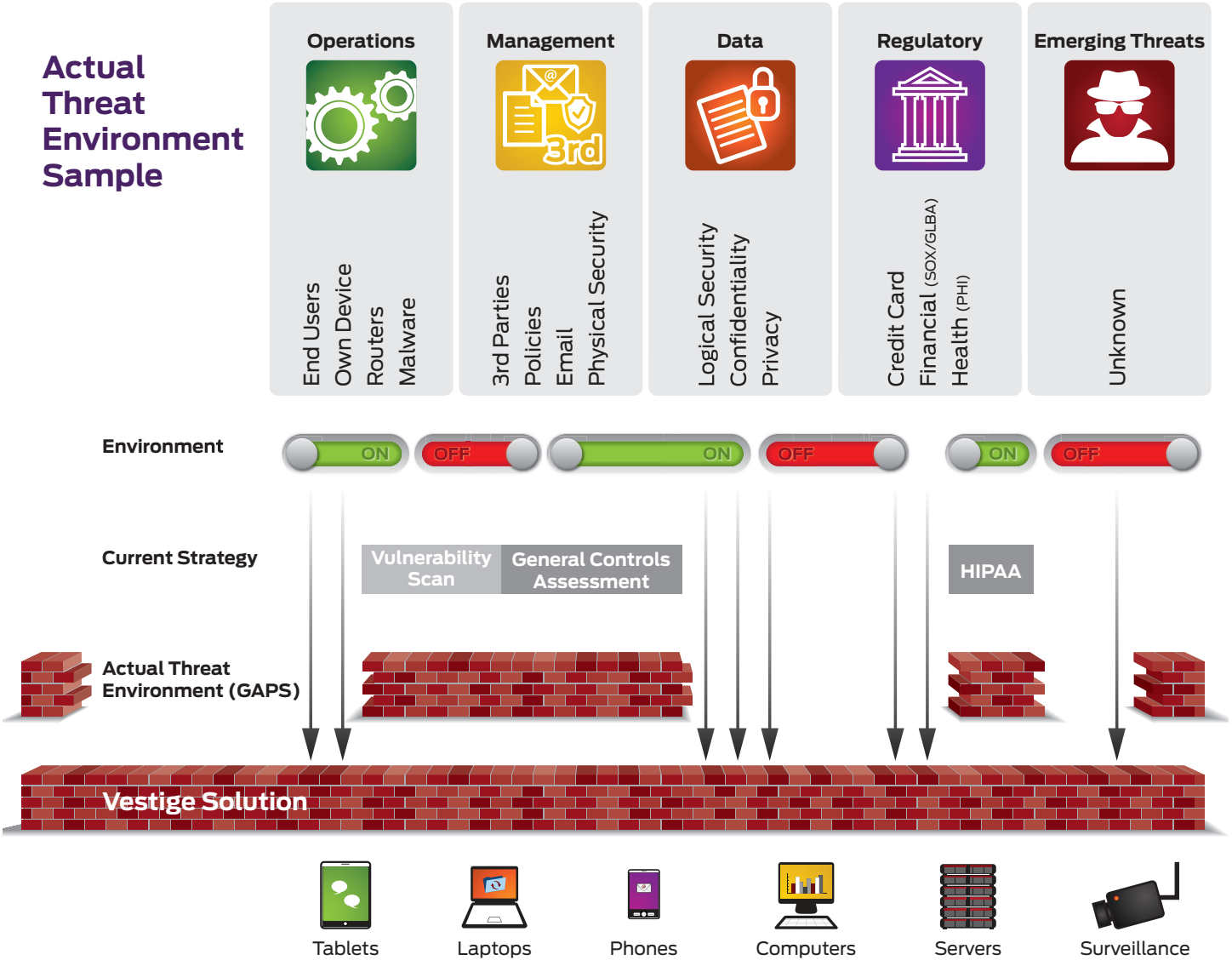
Controls and Your Actual Threat Environment™

The Key to Managing the Risk of Data Breach

The only way in which an organization can effectively and competently manage the risk of data breach is to maintain internal controls that match its Actual Risk Environment™. Anything less — including being merely compliant with applicable regulations — invites a false sense of security and insures that eventually, the business will need to deal with a data breach.

The latest research by Ponemon Institute, Verizon and others shows that the threats not addressed by typical internal controls are leading causes of data breaches, including contractor negligence, third party mistakes and employee errors.

Within this Actual Threat Environment™, Vestige's holistic approach to data protection addresses all these risk factors and extends the analysis beyond any single department and any single area of focus.



Value Provided by Unique Perspective

For more than a decade Vestige has worked closely with Fortune 1000 companies, major law firms and insurance companies to prevent and remediate data breaches. Our forensic and legally trained experts conduct investigations and forensic analysis, and provide Expert Testimony regarding the cause/sources of data breaches. This experience has given us an unique blend of investigatory, IT, networking, law, forensics, and testifying capabilities necessary to provide data breach prevention solutions that provide an organization with meaningful and strategically sophisticated gap analysis between Internal Controls and their Actual Threat Environment™.

The Benefits of Working with Vestige Digital Investigations

- Focus on a layered approach to security that address the Actual Threat Environment™
- Leverages our Deep Investigative Knowledge gained through our experience in helping organizations recover from 'What's actually happening in the real world'.
- Actionable, easy-to-understand, prioritized recommendations to increase the security of your entire IT ecosystem.

Understanding an Organization's True Vulnerability

Looking at the Legal, Social and Business Environment

Vestige's Assessments and IT Reviews are based upon the belief that an organization's true vulnerability for data breach is a function of the company's legal, social, and business environment. We determine the scope of an organization's Actual Threat Environment™ by reviewing and understanding the following :

- The industry, business strategies and operations structure of the company
- The scope of the organization's technical capability
- The social/HR/employment environment that supports the organization
- And all others risks to data presented by the social, legal and organization's environment

Risk Centric Analysis

Because Vestige's Actual Threat Environment™ analysis is risk-centric and not data-centric, our data breach prevention assessments and review are effective for all types of regulated and non-regulated data including:

- Corporate trade secret information
- Personally identifiable information
- Patents
- Personal Health Information
- Financial Information
- Social Media
- Data resident on all sources of corporate owned and relevant personal devices such as cell phones
- Data resident on all relevant devices owned by various trusted business partners

The Result

The result is the only complete assessment that identifies an organization's Actual Threat Environment™, compares it to the organization's Internal Controls (including all controls in place to comply with applicable regulations, such as SOX, GLBA, HIPPA, PCI, etc.), and provides a gap analysis needed to effectively understand and manage the risk of data breach within the organization's real world Actual Threat Environment™. *(See our list of proactive CyberSecurity services on back.)*

CyberSecurity

Choose the Solution That Best Meets Your Needs

The Key to Managing the Risk of Data Breach

Vestige Digital Investigations offers clients several data breach prevention services to choose from primarily based upon the level of validation they wish to achieve surrounding their Actual Risk Environment™ and operating Internal Controls.

Our Assessment Solutions

CyberSecurity Readiness - This is utilized to assess your Actual Threat Environment™ to make sure your organization is well-positioned so the basics are covered — it helps to eliminate the 'low-hanging fruit' that makes it easy for attackers to breach your system. Once implemented this discourages most attackers and they move on to easier targets.

Vulnerability Scanning - This involves running programs designed to assess computers, computer systems, networks or applications for weaknesses. It looks at the outside of an organization's electronic perimeter to determine if it is secure. We then notify where there is an exposure to any known vulnerabilities.

External Penetration Testing | Attack & Penetration (A&P) - In an attempt to find gaps, Vestige performs white hat expert ethical hacking attempts to your IT environment to see if we can compromise the perimeter of the system from the outside, so that organizations can place more secure systems in place to prevent a real threat.

Compliance Audits - We assist organizations in preparing for Internal Regulatory Compliance Reviews with pre-audit readiness reviews to help you learn what the gaps are prior to having the following audits performed:

- Payment Card Industry (PCI)
- Health Information Privacy and Portability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Family Education Rights and Privacy Act (FERPA)
- Assistance with SSAE16 / SOC Reports

I.T. General Control Audits - A comprehensive assessment of the general I.T. control environment.

- Logical Security
- Physical Security
- Development
- Change Management
- Environmental Controls
- Overall Management

Whether your requirements include understanding your current risk, establishing a risk posture, baselining your existing controls or looking for in-depth findings and recommendations on managing and securing your Information Technology assets, Vestige's professional IT Assessment Team can assist in delivering impactful findings and recommendations tailored to your needs.

Contact Vestige today to discuss your CyberSecurity needs.

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