Device & Data Protection

Our reliance on electronic information boosts productivity and lowers the cost of collaborating and managing quantities of information. Yet that reliance exposes costs and risks unacceptable in today's competitive environment. Trends in connectivity, mobility and data breach legislation demand solutions quite different from those that sufficed in the recent past. DriveStrike provides a comprehensive data-protection solution to address these needs in our new environment.

Contents

(877) 375-2468
sales@drivestrike.com

DriveStrike BY SPEARSTONE

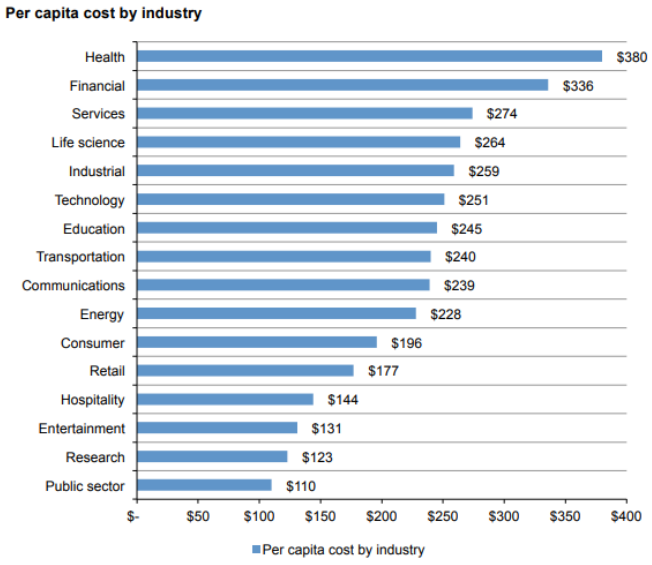
www.drivestrike.com

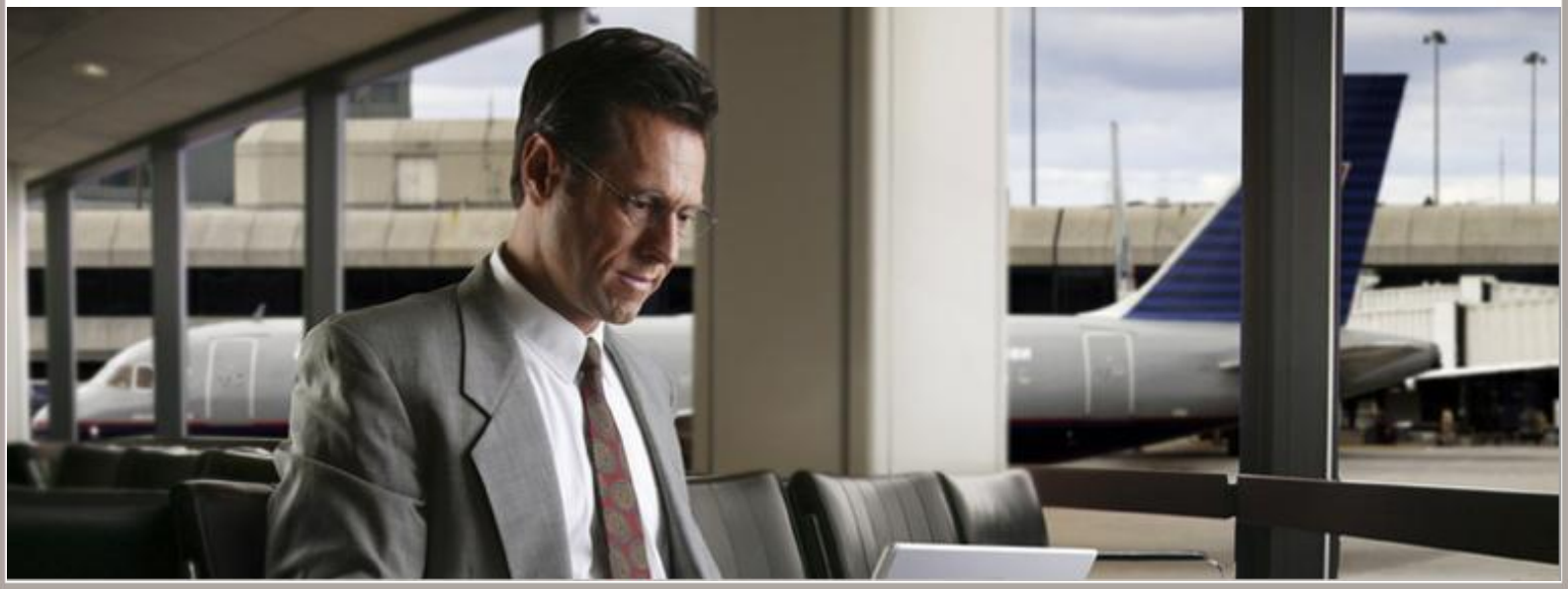
Executive Summary

For many organizations, electronic information is the single most valuable asset outside personnel. Protecting that asset from breach or compromise - the exposure of critical information to unintended parties - is tantamount to protecting your business.

Today's data environment is no longer confined to an organization's local network, presenting new challenges and opportunities for data-protection. With laptops now the most common computers sold, an organization's critical information is spread across more working locations and schedules than ever before. Compounding the data-protection challenge, smartphones and tablets increasingly carry copies of personally identifiable information (PII), protected health information (PHI), work email, contacts, sales data, financial data, insurance information, and documents.

Data breach costs an average of $225 per record. How many records do you have?





(877) 375-2468
sales@drivestrike.com

DriveStrike BY SPEARSTONE

www.drivestrike.com

Data Compromise

The persistence of data - in the wrong hands - can be as costly as its loss. How much of your electronic information would you want a competitor, identity thief, or any unauthorized person to have? What customer records, accounts, contacts, and financial documents would you be comfortable with them seeing?

The consequences are sufficiently grave that seasoned regulations such as HIPAA for healthcare, PCI-DSS in financial services, and FRCP for any company in a lawsuit specify requirements and best practices for handling data and preventing compromise. Newer legislation increases the stakes. Forty-six states now have data breach legislation, requiring that organizations publicly disclose incident details, and inform parties whose personal information is compromised.

According to the Ponemon Institute, a typical data breach in the US costs organizations an average of $225 per compromised data record. The biggest component of that cost is lost business. A third of breach cases involve lost or stolen laptop computers or smartphones, in 2017 the average total cost of a data breach measured in at $7.35 million.

Hardware Loss

$49,246. That's the average cost of a lost laptop after accounting for replacement cost, detection, forensics, data breach, lost intellectual property costs, lost productivity and legal, consulting and regulatory expenses. Of course the computer replacement cost is a small proportion of that total, so why sweat the hardware? Because, it may represent a repeatable pattern whose root-cause you must uncover to prevent a recurrence, such as deficient building security, or a problem employee. Tracking and recovering lost computers and smartphones helps identify such causes, and prevent a repeat occurrence.

Comprehensive Data & Device Protection

These risks highlight the need for a comprehensive data-protection solution combining remote data wipe and hardware tracking. DriveStrike by Spearstone addresses these needs in a manner that works the way today's organizations do, to deliver enterprise-level data-protection at a fraction of its traditional cost.

DriveStrike involves lightweight software installed on devices to be protected and a web-based management portal providing device and data protection across Windows, MacOS, iOS, and Android within one secure centrally managed solution. Administrators can balance central administration and user autonomy according to their needs. DriveStrike uses a Software-as-a-Service model, so it requires no additional IT infrastructure, is highly scalable, and can be easily and rapidly deployed.

The average cost of a lost and breached laptop is $49,246.

Remote Wipe

Almost every organization has had a smartphone or laptop lost or stolen. What's troubling is that 71% report that it resulted in a data breach.

DriveStrike provides protection from data breach by allowing users to remotely wipe sensitive data from their hard drives on-demand. From DriveStrike's secure login site, customers initiate a remote-wipe. As soon as their lost or stolen machine connects to the Internet, it begins executing the remote wipe action.

(877) 375-2468
sales@drivestrike.com

Wipe Data. When a delete is performed, most operating systems do not actually remove the contents of a file. Instead, they simply remove the file system's reference to the file because it is faster. The data actually remain on the drive, and until overwritten, can be read by software that reads disk sectors directly.

DriveStrike's first remote wipe option addresses this risk by overwriting data according to the U.S. Department of Defense specification for secure delete.[1] This approach overwrites each file three times before deleting it, so it cannot be recovered, even by digital forensic experts.

Tests show this approach requires approximately 35 minutes to securely wipe 50 GB. As a result, DriveStrike applies this wipe option only to files a user has backed-up within DriveStrike. If your laptop is recovered the next day, you can recover exactly what was deleted by performing a DriveStrike restore.

Destroy Drive. When a user believes that time is critical in erasing his data, the DriveStrike Destroy option can be employed to render the entire drive unusable in just a few seconds. The Destroy option renders a drive unbootable, and unmountable to be read as a secondary drive in another computer. This makes its data out of reach of everyone except for experts utilizing digital forensics tools to recover data.

For those who want to combine both options, DriveStrike also provides an option to Wipe Data immediately followed by the Destroy Drive action.

Deadman Switch. Our patented deadman switch technology kicks into action if a lost or stolen device is hacked offline and booted. In many data theft situations the thief knows that they cannot boot the PC and connect to the internet. When the thief alters the credentials on the PC and boots the machine our deadman switch challenges them to authenticate, failure to authenticate or connect to the internet automatically invokes a system wipe.

Geofencing. Administrators can define geo-location rules that invoke a system wipe when a DriveStrike protected device leaves a specific location. This capability ensures that authorized personnel do not accidentally leave the workplace with sensitive computing devices and the data contained therein.

Hardware recovery

Ninety-two percent of IT security practitioners report that someone in their organization has had a laptop lost or stolen[1]. And with the all-in cost of each loss ($49,264), you can't afford not to track each down.

DriveStrike can track a lost computer by activating forensic data gathering component within its software. To be activated, users must complete an electronic request and provide a copy of a police report detailing the loss. Once activated, DriveStrike works with Internet service providers and local law enforcement where your report is filed to recover your computer.

DriveStrike's security measures exceed HIPAA, SOX, PCI-DSS, State and Federal data protection requirements.

Organizational Deployment

While DriveStrike provides an easy wizard-based setup for user installations, it also supports enterprise deployments through a command-line based installation that can be invoked from Active Directory, LANDesk, BMC, or other enterprise software management tools

Command-line installs can be tailored to optionally display the user interface during or after installation, and can be configured for a particular user, thereby prevent any device registration dialog from appearing when DriveStrike launches the first time.

(877) 375-2468
sales@drivestrike.com

A partnership you can trust

Spearstone started in 2005 with a commitment to innovation and continuous improvement in data-protection. It drew on deep experience building solutions for Fortune 500 teams in legal, financial and professional services, as well as small-office users in healthcare and related fields. DriveStrike is the expression of its goal to deliver the protections large enterprises enjoy with the affordability that smaller professional organizations require.

Our drive to be the best-in-class commits us to providing a level of service that you'll notice. We seek and act on customer feedback, as we consider you the most qualified judge of our success.

(877) 375-2468
sales@drivestrike.com