The Devil You Know:

MITIGATING INSIDER SECURITY THREATS

JILL SINGER

Former CIO, National Reconnaissance Office
CEO, Tummler Singer Associates
Partner, Deep Water Point

SPONSORED BY: HYTRUST Cloud Under Control & carahsoft.

“When something happens, it is often discovered too late, simply because organizations do not have the necessary policies and safeguards in place to prevent the action.”

Executive Summary

THE DEVIL YOU KNOW: MITIGATING INSIDER SECURITY THREATS

The old adage "trust no one" is particularly appropriate to today's data- and cloud-driven organizations. It applies not only to external threats, but privileged internal personnel as well. In fact, according to analyst firm Forrester, 36 percent of breaches stem from inadvertent misuse of data from employees[1].

With a few unintentional (or intentional) keystrokes, insiders can:

- Gain access to proprietary data, including names, addresses, social security numbers, visa and passport information, tax payments/disbursements, and more;
- Leak top secret, proprietary information, resulting in massive national security compromises;
- Compromise PCI-DSS (Payment Card Industry Data Security Standard) by capturing or leaking account information.

Further, the move to virtualization and the cloud is increasing security risks for government agencies. While these technologies offer great benefits, they also provide simple, one-stop access to applications, data, and other critical tools—making it easy for everything to be compromised in one fell swoop. Moreover, many administrators—weaned on traditional IT—are still trying to fully grasp how to manage virtual technologies, which increases the potential for accidental misconfiguration that could lead to downtime or data breaches.

Virtualization and the Cloud

WHERE RISKS CONGREGATES

Many organizations' security efforts have remained focused on applications, operating systems, and data stores, rather than the virtual layer underneath. But not shining a spotlight on the virtual stack means that all of the things that exist within it—including hypervisors, storage, and more—are vulnerable. These components are often overlooked and not closely monitored.

Agencies relying on public clouds face even greater uncertainty, particularly when it comes to the security of their data. Agencies need to ensure data is not accessible to their cloud providers; however, many are uncomfortable using cloud providers' encryption methods and are unable to demand different encryption approaches to increase confidence.

In short, organizations have granted virtual and cloud administrators the keys to their kingdoms. As a result, this privileged group of insiders often has unfettered access to nearly everything that makes an enterprise what it is. As a result, the privileged insider can—intentionally or unintentionally—put the entire organization at risk. And when something happens, it is often discovered too late, simply because organizations do not have the necessary policies and safeguards in place to prevent the action or the necessary granularity of visibility and auditing to validate what happened.

Gatekeeping

IMPLEMENTING LEVELS OF CONTROL

Organizations must implement some level of gatekeeping to ensure that unauthorized breaches do not take place—a virtual stoplight of sorts. The solution should be automated and designed to recognize whether a request meets defined corporate policy. If it does, the light turns green and the request is granted. If it does not, the request is denied, full stop.

This gatekeeper approach can:

- Prevent misconfiguration, a top perpetrator of system downtime. Downtime can potentially impact hundreds of thousands of virtual machines, in the process costing federal agencies millions of dollars, hours of productivity, and, potentially, the loss of critical data.
- Ensure complete compliance with regulations pertaining to sensitive information. This is especially critical for federal, state and local agencies, as well as healthcare and educational organizations that must adhere to certain mandates.
- Prevent data theft by putting controls in place to ensure sensitive virtual infrastructure can't be copied or moved without secondary approval, and keep data encrypted so that it is unusable if it ends up in the wrong hands.

INSIDER THREAT RISK SCENARIOS

Access to Administrator Credentials

A major online retailer suffered a breach that allowed hackers to access user passwords. The hackers used employee login credentials to retrieve data from the retailer's network. It took two weeks for the retailer to realize the breach even occurred. The retailer was forced to initiate a massive and swift response that involved requiring millions of customers to change their passwords. It also resulted in renewed cries for multi-factor authentication and highlighted the need for additional levels of control.

Phishing Attack

A recent Verizon report claims that 58 percent of cybersecurity incidents in the public sector are caused by employees[2]. Indeed, an employee was at the root of a recent attack on a state Department of Revenue network that resulted in millions of bank account numbers and tax returns being stolen. The attack began when the employee became the victim of a phishing attack, allowing hackers to leverage employee access rights to gain entry into the department's databases. The state was forced to pay for credit monitoring and identity theft protection for millions of taxpayers.

User Negligence

Tens of thousands of employees at a major government agency recently had their personal information compromised. Details about the individuals were left on an unencrypted laptop, which was stolen from an employee's car. The negligence of the employee cost the agency many cycles in trying to retrieve the information—not to mention the goodwill of the agency's employees.

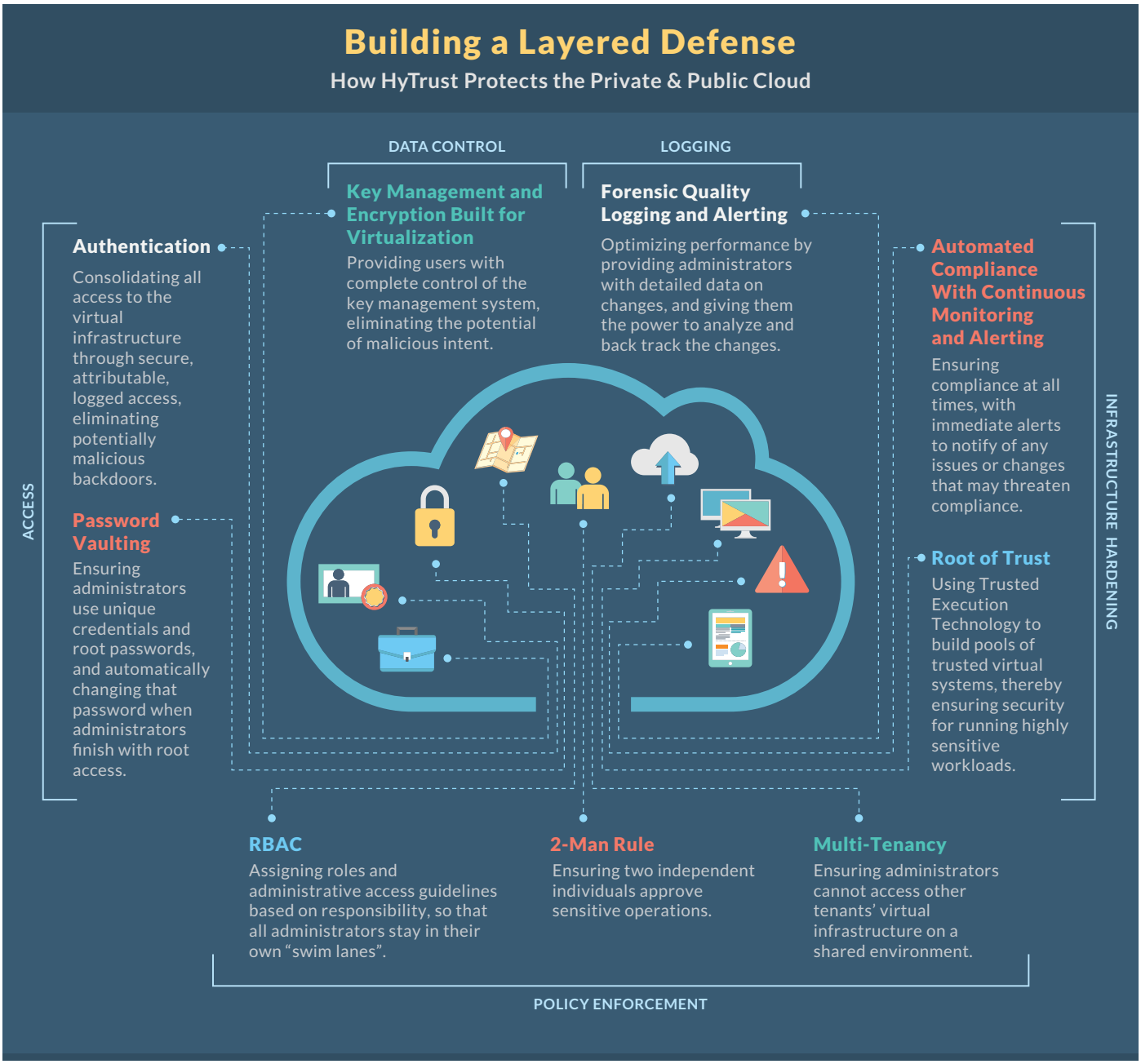
Unauthorized Access to Virtual Machines

A disgruntled former administrator for a pharmaceutical firm created havoc by remotely accessing the virtual infrastructure and deleting 15 virtual hosts, which took down more than 80 production applications. The attack froze the company's operations for several days, disabling email communications, shipping processes, and more.

Protective Solutions

HOW HYTRUST HELPS

HyTrust's solutions provide protection, reduce risk, and improve overall information assurance awareness. The company's highly configurable solutions intercept all administrative requests, determine whether or not the requests meet defined corporate policies, and permit and deny the requests as appropriate. In short, they offer a critical layer of protection—without adding high cost.



Protective Solutions

HOW HYTRUST HELPS *(continued)*

The products also positively impact agencies' bottom lines in other ways. Consider the recent case involving an arm of the military. Hackers were able to steal usernames, passwords, email IDs, and more, mainly because the branch did not validate input into their Web applications. HyTrust's products ensure that organizations do not experience such a profound impact, thereby avoiding unnecessary clean-up costs.

Further, while customers purchase HyTrust products to virtualize even Tier 1 applications and meet compliance and audit requirements, they also use the solutions to enable logistical infrastructure segmentation for multi-tenancy. This approach can reduce costs, improve efficiencies, and produce a large return on investment, because it allows organizations to consolidate both their data centers and servers. While HyTrust's solutions may not provide a 100 percent guarantee against a security breach, they remain critical assets for a layered defense approach.

Layers of Defense

CONCLUSION

As of the publishing date of this white paper, Privacy Rights Clearinghouse has recorded more than 4,000 breaches accounting for nearly 1 billion records. Those numbers are growing daily.

The good news is that many of these threats, particularly those that originate internally, can be controlled. Much like the military requires several individuals to verify launch codes before an attack, organizations simply need to take away the omnipotent capabilities of administrators. Organizations can do this by adding additional layers of verification, encrypting all data, and gaining awareness of all administrative activity. Doing so can help prevent the havoc resulting from a malicious insider or a few seemingly innocuous keystrokes.

[1] Understand the State of Data Security and Privacy; Heidi Shay, Stephanie Balaouras, Brian Luu, Kelley Mak; October, 2013; http://www.forrester.com/Understand+The+State+Of+Data+Security+And+Privacy+2013+To+2014/fulltext/-/E-RES82021

[2] 2014 Data Breach Investigations Report; April, 2014; http://www.verizonenterprise.com/DBIR/2014/

ABOUT HYTRUST

HyTrust is the Cloud Security Automation company. It is backed by top-tier investors VMware, Cisco, Intel, In-Q-Tel, Fortinet, Granite Ventures, Trident Capital and Epic Ventures; its partners include VMware, VCE and Vblock, Symantec, CA Technologies, McAfee, Trend Micro, Splunk, HP Arcsight, Accuvant, RSA and Intel.

For more information, contact Harold Hinson at **hhinson@hytrust.com** or 410-703-5290; or Eric Pankau at **eric.pankau@carahsoft.com** or 702-230-7411; or visit **www.insiderthreatreport.com**.

ABOUT THE AUTHOR

Ms. Jill Tummler Singer is Federal CIO Emeritus and CEO for Tummler Singer Associates, LLC, a small, woman-owned consulting firm. She is also a partner at Deep Water Point, a leading consulting agency. An executive leader with 27 years of federal support in the areas of transformation, strategy, leadership, and technology, Ms. Singer's last federal assignment was the CIO for the National Reconnaissance Office where she was responsible for Information Technology, Assurance, and Management.

Prior to joining the NRO, Ms. Singer served as the Deputy CIO for the CIA. Throughout her federal career, she served in several senior leadership positions including Director of the Diplomatic Telecommunications Service, U.S. Department of State; and Chief of Systems Engineering, Architecture, and Planning for CIA's global infrastructure organization. She held industry positions with SAIC, Inc., GE Aerospace, and IBM.

Ms. Singer can be reached at **jill@tummler-singer.com**.

The Devil You Know:
Mitigating Insider Security Threats

Written by: Jill Tummler Singer
Former CIO, National Reconnaissance Office
CEO, Tummler Singer Associates
Partner, Deep Water Point

Sponsored by: Carahsoft® & HyTrust®

HYTRUST Cloud Under Control carahsoft®