Top 3 information security investments for 2015.
TABLE OF CONTENTS

Introduction 2
Physical access controls 2
Logical access controls 3
Identity authentication solutions 4
How MicroStrategy Usher addresses all your investment needs 5
  Physical access control 5
  Logical access control 5
  Identity authentication solutions 5
Introduction

While it may sound paranoid, the threat of industrial espionage today is all too real. It seems that every day another company’s confidential information is hacked—and the cost of these security breaches is escalating at an alarming rate. According to a study conducted by the Ponemon Institute, the average cost of an information security breach to a U.S. company is $3.5 million; this figure doesn’t even include the mega-corporations who were most recently the victim of an attack.

What the Ponemon figure also doesn’t represent is the post-attack cost to a company’s reputation. We all know public trust is a key requirement for revenue and business continuity. Reputation can be a company’s biggest value driver, or its worst enemy. For one highly visible retailer, the latter came true in 2014. This name-brand retailer estimated that in Q2 2014, the costs associated with their security breach exceeded $148 million. Forrester Research Analyst John Kindervag suggests that over time, those costs could eclipse $1 billion.

The moral of the story: your information is too valuable to be protected by traditional and outdated security measures.

As a result of these trends, businesses of all types are making 2015 the year of information security, or InfoSec. In this paper we outline three investments organizations must make to ensure they’re secure. After reading, you will understand what makes your company vulnerable to information security breaches and what investments you must make to resolve these vulnerabilities.

Physical access controls

Of the three investments outlined in this paper, physical access controls are perhaps the least evident. Most companies utilize various forms of physical locks and keys for access control; these solutions have obvious weaknesses. These weaknesses do not, however, stem from the solutions themselves. Rather, they are the result of the user.

Studies have shown that the top threat to an organization’s data is its own employees. In fact, it has been reported that 69% of serious organizational data leaks are caused by employee activities—both malicious and non-malicious in nature. With activities of malicious intent, these leaks are often a result of employees physically accessing server rooms and devices that contain sensitive information. In these situations, physical access controls are either abused or, even worse, non-existent.

The most infamous information security hack of 2014 is a poignant example of failed physical access controls. According to the hacker group responsible, they were able to obtain their victim’s private information by leveraging employees on the inside with physical access to the target network. If this is true, it implies employees physically injected a virus into the network that enabled the hackers to access their victim’s data remotely. Additionally, if the hacker group did in fact leverage employees, then it will be very difficult for the victim to recover fully. As CSO Online points out, "physical security related breaches… are hard to contain and recover from"
because evidence can be tampered with or simply removed.”

What makes this story even more worrisome is that the employees were said to have “similar interests” to the hacker group. No organization wants to believe their employees are capable of being adversarial. However, it is nearly impossible for an organization to prevent the possibility of a bad egg—there’s always the risk of a disloyal or embittered employee attempting an information security breach. When this happens, it is critically important that your company has suitable physical access controls to prevent a breach.

So what can your organization do to prevent a physical security-related attack? Most importantly, consider how your employees currently access your physical computer network environment. Is it with the turn of a key? Is it an electronic key fob? Is there an actual guard standing at the door? All of these methods lend themselves to human error. Physical keys or key fobs can be lost or stolen. A guard can mistakenly grant access to an unauthorized person.

Every organization needs a physical access control solution that authenticates individuals based not only on something they have (such as a key, key fob, or physical badge), but also on something they know (like passcodes and PINs), and something they are (biometrics). From the user’s standpoint, the access tool needs to be difficult to lose, steal, and replace.

**Logical access controls**

While the biggest information security threat to your organization may be your own employees, logical access controls ensure only appropriately credentialed employees have access to your workstations, applications, and information networks. Unfortunately, at many companies employees across the organization have unhindered access—typically “resolved” by controlling access via passwords.

Here’s an alarming statistic: 76% of all cybersecurity breaches are caused by weak or compromised passwords. Equally striking, it costs your firm anywhere from $51–$147 every time someone needs a password reset. This cost is driven by the number of calls your help desk fields exclusively for password resets (Fact: 30% of all help desk calls are a result of forgotten passwords). Standard logical access controls like passwords are surprisingly expensive to your firm—even without a breach. By relying on passwords, your organization is leaving itself vulnerable to even greater costs, as passwords are easily hacked by internal and external threats alike.

It is critically important for your organization to secure its sensitive information using effective logical access controls. Essentially any access control utility that relies on simple data entry—including passwords, PINs, and knowledge-
based questions—is not enough. Security measures like these cannot account for the person inputting the data. Much like physical security platforms, logical access platforms must leverage the person’s true, non-replicable identity.

### Identity authentication solutions

As greater emphasis is placed on improving physical and logical access controls, it becomes increasingly important to manage these controls centrally.

Information security is simply too important to be directed by individual departments. Distributed ownership leads to unclear accountability, making it difficult to identify security vulnerabilities and breaches without a single unified platform. This trend toward centralized administration is called converged access management (CAM). CAM is the ideal that every organization must strive to achieve.

However, CAM is all but impossible to achieve when employees are forced to use different forms of identification for different types of authentication purposes. If employees use a physical badge to gain physical access and a password to gain logical access, it is highly likely that separate administrators manage each type of access. Organizations in this position sacrifice both efficiency and security.

To guarantee the best protection, organizations must adopt a single, comprehensive identity authentication solution. For employees, this means a single authentication tool that is simple to use. For administrators, this means an authentication platform that is difficult to defeat and doesn’t require a specialized skillset to manage. And crucially, the identity authentication solution must provide comprehensive threat monitoring and analysis.

### How MicroStrategy Usher addresses all your investment needs

#### Physical access control

With MicroStrategy Usher, physical access is no longer based on possession of a physical badge or key without regard to
identity. By interoperating with the world’s most prevalent physical access systems, physical entry points can be controlled using encrypted digital keys attached to a mobile device. These digital keys can be remotely distributed and revoked in an instant, and can only be accessed by providing three factors of authentication—your phone, your phone’s passcode, and your fingerprint. Most importantly, you can monitor and record who accesses each entry point at any given time—providing unparalleled insight into potential internal threats.

**Logical access control**

With MicroStrategy Usher, you are no longer vulnerable to password and pin-related cyber breaches. Moving beyond traditional logical access security measures, Usher enables users to log into workstations as well as web, cloud, and mobile applications with just their mobile device. Not only does Usher eliminate the hassles and potential costs associated with passwords and PINs, but it also delivers single sign-on (SSO) for SAML-enabled and mobile applications. It’s simple to use, seamless to integrate, and is capable of securing the entire enterprise.

**Identity authentication solutions**

MicroStrategy Usher makes converged access management possible. Employees can securely authenticate their identity anytime, anywhere. Regardless of whether they are trying to access a physical entryway, a web/cloud/mobile application, or simply confirming their identity face-to-face, all they need is their mobile device. By using the Usher Network Manager, enterprise security administrators are able to manage an organization’s electronic badges, keys, and permissions in one place. Usher gives security administrators a 360-degree view of their network—affording administrators the ability to detect and deter information security threats of every type.

**MicroStrategy Usher: Three powerful solutions in one**

**Usher Security**

*All employees, vendors, and customers*

The key to unlock your enterprise. Replace badges, passwords, physical tokens, and keys with an app. The security badge allows identification, logical access, physical access, and transaction authorization.

**Usher Mobile**

*Sales reps, field service, managers, and executives*

Information at your fingertips. Personalized and localized intelligence about resource utilization, transaction authorization, and all other activity in the enterprise.

**Usher Analytics**

*Analyst, data scientist, administrators, and database architects*

The platform for building custom reports. Combine access and authorization data with all other data sources within the organization for performance insights.