Securing Executives and Highly Sensitive Documents of Corporations Globally

Best Practices and Use Cases

www.gemalto.com

gemalto

security to be free

Table of Contents

Securing Executives and Highly Sensitive Documents of Corporations Globally

Best Practices and Use Cases

For IT professionals up against the significant challenge of keeping corporate networks and information secure, top level executives and board members present unique requirements. Highly mobile and highly privileged, these individuals typically have access to the enterprise's most confidential information, from earnings outlooks to acquisition plans to new products.

The potential profitability to hackers of this information makes executives prime targets worthy of significant time and resource investments.

There are many risks. Data can be leaked if a laptop or mobile device is lost or stolen. Login credentials can be compromised by "spearphishing"—an attack mounted against a high value target, perhaps over a period of several months, blending customized phishing emails, password-stealing crimeware unique to a specific target and social engineering. An employee at an external director's firm could commit insider fraud there, without even touching your network.

The goal of this white paper is to give an overview of the problems associated with protecting information for mobile executives, and consider potential solutions.

As the global leader in digital security, Gemalto ships approximately 1.5 billion smart secure devices every year and supplies a wide range of software and services to hundreds of the world's largest enterprises and government agencies. Our solutions help banks and mobile network operators ensure billions of transactions every day are securely conducted between the right parties. They power ID documents that are practically impossible to forge. And they allow people exchange information and access networks without fear of being spied on or hacked.

Drawing from our extensive knowledge and experience, we hope the information shared in this guide will empower you to find actionable ideas that you can use to implement highly resilient and effective information security for your organization's mobile executives.

IT challenges

The IT team is responsible for protecting the security of information for their mobile executives and must consider a wide range of security risks and challenges.

Common threats to IT security

1 **Lost or stolen devices:** Americans alone lost approximately $30 billion worth of mobile phones last year, with half of them used for both business and personal activities. A Ponemon Institute study of U.S. corporations reported a laptop is stolen every 53 seconds. There is an evident risk that these devices can contain confidential company information or be used by hackers to gain access to IT systems. In fact, Ponemon estimates the average cost per lost laptop is $49,000 due in large part to the high cost of lost intellectual property.

2 **Compromised login passwords:** Remote access and authentication in many enterprises still rely on insecure usernames and passwords to verify identities and authenticate users. Hackers use phishing emails to install Trojans, keyboard loggers and other malware to attempt to steal user credentials.

3 **Spearphishing:** High value senior executives can be singled out for a long lasting campaign to compromise their logins or systems. This can include mining social media sites to get password clues or creating very credible, personalized "spearphishing" emails that can lead to compromising an endpoint with crimeware.

4 **Custom zero-day attacks:** Using sophisticated toolkits like SpyEye, hackers can create new variants of Trojans easily, even creating a unique threat for a specific target executive. The problem is that many endpoint defenses, like antivirus and firewall, rely on a signature to detect crimeware, meaning they cannot stop new threats they have not seen before.

5 **Mobile malware:** According to Juniper Research, mobile malware more than doubled in 2011. It grew by 155% across all platforms—Apple's iOS, Research In Motion's BlackBerry and Symbian. Note this does not include the Google Android platform, which in the last seven months of 2011 grew by an astounding 3,325%. Hackers are targeting the mobile OS, the Web browser, the means of communications, the client applications and the user behavior. Mobile malware uses all of the same techniques as with desktops or laptops: Trojans, dialers, phishing, malicious sites, spoofing, and man-in-the-middle. The malicious attacks may result in identity theft, unauthorized access to confidential data, altered data, unwanted phone calls or denial of service.

6 **Rogue apps:** The fact people can choose their own apps for mobile devices, many at no charge, is a dream for hackers and a nightmare for IT security; Get Safe Online, a public service organization backed by the UK's Office of Cyber Security and Information Assurance, found malware apps aimed at mobiles grew by 800% in just four months of 2011, and Russian security researchers at Kapersky Labs found 34% of Android malware tried to steal personal information.

It can be months or even years before you know a hacker has gained access to your network. In the case of one significant telecommunications company, hackers enjoyed nearly a decade of undisturbed access to business plans, company emails, research and development reports and technical papers. The intrusion was caused by the theft of passwords from seven company executives. Executives are at the highest risk because they commonly have near unlimited access to the most sensitive data and company information.

Sensitive information lost on a company computing device exposes the company to financial and reputation damage when reported and losses are often immeasurable.

Security risks are not the only problem IT management faces in protecting senior executives. This group is highly mobile, extremely busy and often not very comfortable with personal technology. Any techniques used to help better protect their information and access must be simple, efficient and reliable in addition to being highly secure.

Below you will find some specific examples of use cases and solutions for protecting information for executives that can help keep your company safe from hackers, hacktivists and nation-sponsored espionage.

Stolen Laptops

Reports of lost or stolen executive laptops and credentials are common:

> A stolen laptop of a LinkedIn executive revealed plans for a massive acquisition

> A BP executive lost a laptop containing a spreadsheet with the names, social security numbers, phone numbers, and addresses of 13,000 compensation claimants resulting from the oil spill in Louisiana

> A stolen NASA laptop contained ISS commands used to control the International Space Station

A Sandbox for Secrets

Since a company's board of directors is typically made up of senior executives of other organizations, anytime a board member is sent confidential information about your company, that data becomes vulnerable to leakage on the board member's company network.

Information stored in the board member's mail account or files that are saved on the local server at the member's own company would be vulnerable to snooping by the IT team that maintains the member's emails and servers. It is also well known to hackers that top level email strings can contain powerful information regarding corporate strategy, financial results, product development and customer acquisitions. Corporate secrets such as these can go for big money on the black market.

Additionally, once data is on the board member's server or email, it is also out of your control, and its security is reliant on the measures the member's IT team has taken to secure their own networks. This means your files could be vulnerable to Trojan or other attacks on their networks or endpoints.

Another situation that presents the same risks is laptop security breach at a border checkpoint when traveling internationally. Frequent employee or executive travel exponentially increases the likelihood of his or her laptop being searched when crossing the border. Border agents can accidentally, or on purpose, access sensitive data that may be stored on the laptop, and leak it to their government, or sell it to other companies. In fact, some countries, including the UK and the US have laws that allow border agents to check laptops and detain the devices for extended inspection—which can last for days or even weeks.

One way to ensure all of your data is secure in these situations is to provide board members, executives and employees who travel frequently with a sandboxed workplace that is segregated from the host PC.

A sandbox is an isolated secure workspace that runs separately from the PC, meaning even if the PC is compromised by a hacker, the sandbox remains secure, preventing data loss. When online in the sandbox, the user can access corporate data and applications through an onboard VPN client. When offline, the board member can use onboard applications such as Microsoft Office or Adobe Reader. Administrators can also set restrictions for the sandbox so documents cannot be copied or printed from a remote location.

By issuing a "lite" laptop, meaning only the basic applications are stored on it, as well as the secure sandbox, the user can easily access the information they need, leaving no trace of organization information on the host PC, keeping the your data safe and secure.

Sandboxes can either be downloaded as an application or run from a thumb drive. Running a sandbox from a thumb drive is more secure, due to the fact that you need the drive in order to login and access the sandbox, not just access to the PC.

Email encryption can also be added for additional security for all communications between executives and board members. By using certificate-based smart card security, executives can choose to encrypt any emails containing sensitive information. The cryptographic process within the smart card protects the email so only the intended recipient can decrypt the message. This functionality is easily enabled using a Microsoft infrastructure and productivity tools like Outlook. So even if a board member or executive's email is hacked, sensitive data will be protected from prying eyes.

In addition, you want to be sure official documents are coming from the person they claim to be. Digital signature guarantees the authentication of the person signing the document. Digital signatures are also less expensive, faster and more efficient than "wet" signatures for validation and approval.

Laptop and Device Loss

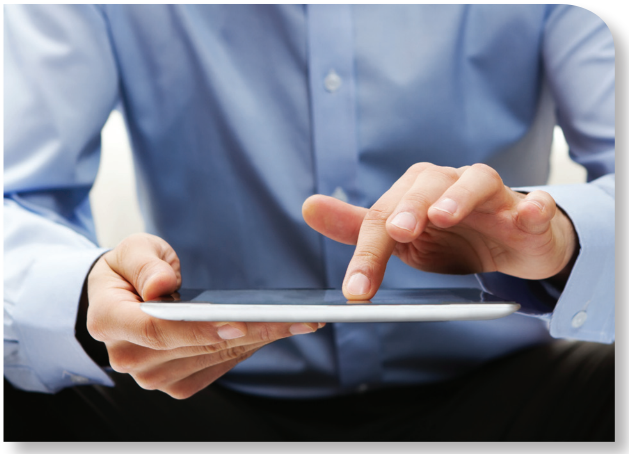
With travel, there are many additional dangers to digital security other than crossing borders. Any time an executive or employee travels or works outside the office they run the risk of losing their laptop. Sometimes the device is left out in the open in a hotel room, unattended in a public location or forgotten when its owner is in a rush. Any time a laptop is stolen or lost, there is a possibility the data on the device has been compromised. This creates a major security risk for companies and could cost thousands of dollars-worth of company secrets, client data, or even access to financial records.

> Any time a laptop is stolen or lost, there is a possibility the data on the device has been compromised.

This is another situation where using a sandboxing device can help keep company data protected. If the laptop is stolen, thieves would still need the portable security device that launches the virtual sandbox. The sandbox, like stated before, allows the owner to access corporate data and applications via the onboard VPN client that provides a secure connection to the company's network by authenticating the device while it is online. Even if the computer is unable to access the Internet, the owner is still able to access onboard applications such as Microsoft Office, Adobe Reader and others.

Another way to keep devices secure, even if they fall into the wrong hands, is to issue a biometric smart card along with pre-boot authentication and hard drive encryption. This requires the user to use a biometric smart card to prove their identity to the computer during booting, making it so only authenticated users can access the laptop.

Mobile Device Breach



In this day and age, everyone wants to be able to use their own devices for work. The bring your own device (BYOD) trend is causing many enterprises stress. Not only does the IT department have to worry about corporately owned desktops and laptops, they now have to worry about employees accessing sensitive data on their smartphone or tablet. The problem is mobile devices can be lost, stolen, and now even hacked and infected with mobile malware.

While mobile devices present a new additional threat to security, the BYOD trend is here to stay. Executives are a prime example, they are constantly on the go and depend on their mobile phone or tablet when they are traveling. This creates more entry points for hackers. Leapfrogging, when hackers gain access through a mobile device and move on to the network when users sync, is becoming more and more prevalent.

In order to lock down and secure email, IT departments can require employees to use a one-time password (OTP) or a PKI-based strong authentication credential to login to Outlook Web Application (OWA) through a browser to prevent unauthorized access to emails on a lost or unattended device.

OTPs are a form of multi-factor authentication, which complements access security based on something you know (the username and password) with something you have, an OTP token. The OTP token generates a one-time password that significantly increases the login security.

Requiring an OTP token to access OWA makes it possible for employees to use their mobile device, such as a laptop, smartphone or tablet, without endangering the security of the information stored in their emails. Even if the device is lost or stolen, the email server will be inaccessible since any would-be criminal who comes in possession of the device would not be able to use it, because they would also need the OTP token to authenticate the login.

The next higher level of strong authentication security is to issue a smart card-based secure element (SE), such as a smart card-based PKI certificate and an associated reader, for a mobile device to secure logins and encrypt or sign emails. Often this works by inserting the smart card into the reader, which then authenticates the card and the user is prompted for a PIN, which when correctly entered confirms the user's identity.

SEs can also be used directly with the authentication server to prove identity. In this instance, the user inserts the smart card into the reader, which is connected to the user's computer and confirms the validity of the card for authentication, the same way a smart ID card can be used to open secure doors in an office.

Another possible authentication factor is to use something you are, a biometric combined with a smart card. This approach is the same, except it replaces a PIN code with a fingerprint biometric. This helps avoid problems with people forgetting their PIN codes—and prevents them from sharing their PIN code and credential with someone else.

Fingerprint biometric systems do not actually store the complete fingerprint. Instead they create a template from the fingerprint image during enrollment, which is used to authenticate the user. Also, the matching is done internally on the smart card using match-on-card technology, which protects it from threats on the PC or user device. Another benefit of match-on-card is that the user always has their biometric identifier with them, securely stored and encrypted on the card, so they are not dependent on network connections for authentication to the card.

Ease of Implementation

One final bit of good news is that provisioning, deploying and using OTP tokens and smart card-based credentials with identity certificates are very straightforward today. All leading IT infrastructure suppliers, including Microsoft, IBM, HP, CA, Citrix, Adobe and many more are already fully supporting the use of smart card-based two-factor authentication. In fact, many of these IT leaders already use smart card ID credentials internally themselves.

If your organization or your clients are primarily operating a Microsoft environment, you can be assured your core infrastructure is ready to evolve into identity-centric security. There is no need to install additional middleware; it is as simple as adjusting some settings and enabling software modules to get started. Key Microsoft components that support smart card-based credentials and certificates include:

- Forefront Identity Manager (FIM): A simplified framework for managing and provisioning user identities, user accounts and access, password and certificate-based credentials such as smart cards, and identity-based policies across Windows and heterogeneous environments.
- Certificate Authority, Active Directory and Active Directory Federated Services (ADFS): Tools for certificate issuance, authentication and access control for credentials and identities.
- Windows desktops and server operating systems: Full support for desktop logins, terminal services and security policy enforcement, as well as self-service provisioning and maintenance with FIM for everyday tasks like PIN resets.
- Applications including Outlook, SharePoint, Office: Login, digital signature and encryption capabilities.
- Office 365: Microsoft's cloud-based apps support the use of smart card-credentials as well.

For Linux and Apple infrastructures, implementation at the desktop level is also readily achieved using off-the-shelf resources. Provisioning can be accomplished using Microsoft's FIM or Gemalto's cloud-based provisioning and life cycle management solutions for example, as well as services from other providers.

Summing Up – Strongly securing information and access for executives is a best practice

Every week brings new stories of companies damaged by the breach of sensitive information, a problem that can be prevented by the best security practices discussed here. Further, much like the early days of the Internet or PCs, new mobile technologies and cloud services are introducing new security risks. Preventing data loss and protecting sensitive information from unauthorized access should be a top concern of every company.

While better security is needed enterprise-wide, it is essential that executives and board members get personalized attention and the greatest levels of information and remote access protection. It is evident that username and password authentication is simply not a secure way to protect the high levels of information within a company to which these executives have access. Using sandboxes, OTPs, smartcard-based multi-factor authentication and biometrics as part of your login and identity verification procedure can prevent data loss and protect your confidential information.

Thank you for reading

The purpose of this brief was to give you an overview of the best practices and use cases that demonstrate how organizations are protecting executives and board members IT access, using sandboxing and multi-factor strong authentication to maximize security to protect the most critical and confidential information in the enterprise.

We hope these ideas help you start planning new possibilities for protecting your executives and employees using strong authentication.

Where do you go from here? To start, we hope you share this brief with your colleagues. Work with your management to make sure they understand the threats and rationale for implementing strong authentication, and what that will do to strengthen the security of your IT infrastructure.

When the time is right, consider contacting us. Gemalto's Protiva family offers a full spectrum of strong authentication solutions, from OTP to PKI credentials in cards or tokens. Our IDConfirm Authentication Server fits simply into your infrastructure, and Gemalto gives you many options for deployment, from enabling your in-house management to cloud-based services for hosting of provisioning on-boarding.

Gemalto has a team of skilled product engineers who can make specific recommendations for your situation, and provide you with more detailed information about what we have to offer and how we work. Do not hesitate to contact us in whichever way suits you best. Contact information for our offices worldwide can be found at http://www.gemalto.com/php/office_search.php.

What did you find most useful? What would you like to know more about? We look forward to hearing your feedback and questions.

IIIII The world leader in digital security

www.gemalto.com

gemalto
security to be free