Endpoint Protector's Guide to

Identifying and Preventing the Top Data and Network Security Threats of 2011

ENDPOINT PROTECTOR

Working safe with portable devices

COSOSYS

OVERVIEW

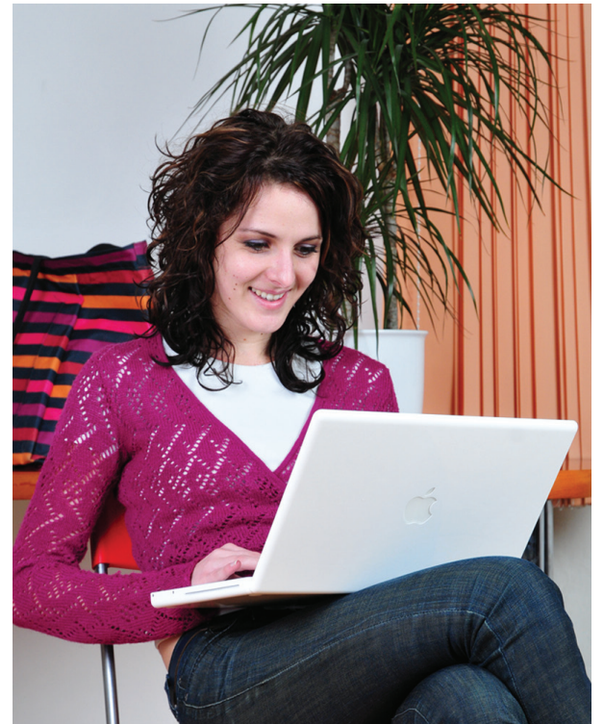
In order to ensure a secure environment in the business and personal worlds, the first step is to properly identify the biggest, most common and most damaging threats and learn what can be done to prevent them. Based on the frequent security breach news, the many reports and surveys published throughout 2010 and our own expertise and ability to identify trends, Endpoint Protector has determined the biggest data and network security threats most companies will have to face in the year to come.

The purpose of this white paper is to introduce IT professionals, business owners, employees and private users to the highly frequent and always threatening risks of the fast-paced, always mobile and always connected age we are living in. To be able to better asses potential damages and optimum prevention methods, it is paramount to familiarize ourselves with potential scenarios, available countermeasures and keep up to date with the latest security trends.

The world we currently live and work in is one where new technologies emerge everyday, powered by a seamless connectivity trend where every new gadget, software, app or piece of equipment is designed to almost instantly become an integrated part of a larger network, be it work environment or household.

Work and personal computers, iPhones and other smart devices, iPads or tablets, digital cameras, music players, they are all quickly synced and connected, making data always available from anywhere on the planet, provided the now basic Internet connection exists. If not, a bluetooth connection or USB connectivity can easily solve our synchronization issues. While it does make us more active and a lot more productive, it also exposes all the data we carry on devices that get smaller by the day to hordes of security perils and standing-by exploits looking for the tiniest way in.

Identity theft, hacking, cyber attacks, data loss, online fraud, lawsuits, fines, these are but a few of the consequences businesses might face when failing to properly manage the security risks they expose themselves to. Each of these consequences translates into money lost in a matter of seconds.



THE TOP THREATS OF 2011

OVERVIEW

There is no greater threat to data and network security than that coming from the inside of a company. The people businesses generally rely on to grow and work together for a profitable outcome often work against them. Staffers lack the knowledge, the will or the moral background to prevent data loss, data theft or other security breaches from happening.

The poorly managed inside threat is one of the most frequent causes for data breaches. Coming in three different shapes, it often results in monetary loss, lawsuits and even imprisonment for the employee at fault. Most insider-caused breaches are powered by one main aspect - companies tend to treat employees differently than outsiders, regardless of how high or low they rank on the corporate ladder. Security is generally looser than for someone outside the staff and the control and monitoring of their actions are close to non-existent or misdirected. Management teams usually worry more about ensuring employees don't waste precious time than about making sure they don't access or expose private company data.

Let's explore some of the most common forms the insider threat manifests itself in.

1.1. Employees with a malicious intent

Some of the people companies hire either start working for them with a clear plan of breaching their security and making profits off their intrusion, or develop it on the way, or are persuaded to help others from the outside gain access to private company records. The phenomenon has spiked during the recession, as many disgruntled or simply hopeless employees turn to data theft to secure some monetary gain or a future position with a competitor. Many don't even realize what they do is illegal, as they consider the results of their work to belong to them and not to the company.

Some of these breaches and their exploitation are only discovered long after they have happened, when the consequences are already monumental. Take the TJX case, one of the biggest data breaches in history, where the tens of millions of credit and debit card details stolen have been harvested over a lengthy period of time, across the entire US and Canada.

With the world far from having escaped the effects of a down-turning economy and the temptation of making a quick illegal buck ever-present, employees displaying malicious intent are here to stay.

1.2 The untrained and careless employee

While no intent of foul play can ever be accused in such cases, the losses they cause are undeniable. Employees make private files public by mistake, they copy confidential data on their portable devices and then lose them or thieves steal them, they let outsiders in and fail to make sure they do not access restricted areas of the company networks and steal their property.

The most common cause of such honest mistakes lies in the lack of proper training and education provided to employees. All staffers need to be told what is proper data usage, what risks they face, how to act when having visitors, what to look for in themselves and in others' behavior. The responsibility for educating the business world and the home users alike falls on employers, companies operating in the security industry and the media.

Another strong cause, that comes from lack of education as well, is the general disregard for security policies. Employees think it is more than OK to circumvent policies and gain access to restricted areas, upper management expect access privileges and looser security rules, although they lack the knowledge to handle them safely.

1.3. Social Engineering

A derived form of the above manifestation of the insider threat, social engineering implies an unknowing employee with little knowledge of what information is restricted and what can be shared with outsiders and a clever and malicious individual that gets them on the phone or engages them in a virtual conversation and obtains valuable information, from business plans to login credentials. Live experiments have shown that it is extremely easy to get plenty of restricted information in half an hour from naive employees.

Again, the main cause is the lack of proper training and the people's general openness to strangers powered by our current lifestyle based on large amounts of trust invested into individuals we meet online and end up calling friends.

2. PORTABLE DEVICES

There should be a way of enhancing productivity, of allowing us to set up a virtual office anywhere in the world, of helping us carry and use data easily and safely. Yet portable devices, from cameras to smart phones and laptops are prone to data breaches. High connectivity, always-shrinking dimensions, easy to steal and lose, all these features make portable devices and the astonishingly large amounts of data they carry prone to exposing private details of companies and individuals.

Misplaced and stolen portable devices are one of most frequent means of having company data stolen or lost. Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan lost about 280,000 medical records together with a misplaced portable drive. Cooper University Hospital experienced a similar incident this year in July. Accomack County exposed the data of 35,000 residents when one of their laptops was stolen from an employee who took a trip to Las Vegas together with his employers property. Another laptop theft endangered the private records and identities of 7,000 City College of New York current and former students. And these are only a tiny percentage of the incidents reported this year alone, with many more kept quiet or never noticed.

Most of the stolen or lost portable drives and gadgets have little or no security in place. No complicated passwords, no data encryption, nothing to stop those aware of the gold mines they contain from using the information they come across.

3. MALWARE INFECTIONS

Worms transmitted through USB connections have been the lead story of this year security world. Conficker, Stuxnet, Donwadup, however they are called, the pattern is similar, they infect networks of hundreds or thousands of computers and then start doing their damage. Stuxnet had such a tremendous impact, it raised genuine concerns of how future cyber wars would be carried. It affected the industrial systems operating power plants and other such complicated structures whose malfunction could lead to disasters. It also raised red flags for cybersecurity departments in each and every powerful country in the world, forever changing cyber warfare plans for the future.

This is just one aspect of the malware world and the most hyped up one, but this threat will be ever present and ever growing. While people have somewhat learned that downloading suspicious attachments, browsing shady sites and file sharing can lead to serious malware infections, they still tend to plug and play just about any device they come across - cameras, USB sticks and other portable devices they find, friends' devices and so on, exposing themselves to some of the most powerful malicious software out there.

4. CYBER ATTACKS AND HACKING ATTEMPTS

Malicious individuals will always try to compromise your system, get in and run havoc within your company's digital assets. While stopping them might sometimes prove hard to accomplish, making sure they cannot gain access to sensitive information might be a lot easier. While firewalls and other methods to keep outsiders far from the business networks are always evolving, data has to be properly encrypted and secured on its own because to this date there is no bullet proof security. Even the Pentagon had to admit a security breach that gave access over US military computers to foreign servers. It indeed took an infected flash drive to first spread malware to an entire military network, but criminals still gained control over the computers in question. The breach, coupled with other intrusions in governmental networks, lead the Pentagon to banning the use of USB flash drives, but they later came up with far more productive security measures.

5. THE THIRD PARTY LIABILITY

In our effort to render everything efficient and automatic, we depend a lot more on third party entities to handle our data: external data bases, hosting providers, credit card payment processors. Companies generally choose them based on the services they provide and their pricing policy, putting their trust into a promise of security they rarely check thoroughly. It is again a question of education in the field of data security and knowing what to ask when assessing the level of protection provided by third parties.

6. EXPLOITS AND VULNERABILITIES

There is no perfect software. Bugs are a given and tiny doors into virtually any system. They are always there, they just need to be found. And the wrong doers are getting better at finding them. If they don't, there are entire communities looking for and exposing such exploits and vulnerabilities. Although it is a commendable effort, it also gives all the wrong information to people who would use it against companies and individuals for their own profit. Everyone knows by now it's important to keep every piece of software up to date, but other than that and maybe antivirus and firewall protection, they have no other backup plan. Access monitoring, enforced encryption for important files, these are still new to most people.

7. SOCIAL NETWORKING

Social networking is not a different kind of threat in itself. Yet it harbors plenty of other threats to become a huge risk on its own. It is the playground for those indulging in social engineering, spreading malware, or stealing login credentials. While most think stopping employees from spending time on social networks is the solution, a better choice is always to train people and teach them how to stay safe. Remember what we pointed out in our section about insider threats - employees often circumvent security policies and still engage in unsanctioned activities online. Rather than restricting access and trying to force them to stay safe, while also tempting them to try and hack their way into the social networking channels, better invest the effort into making sure they know how to act and respond when accessing their social profiles.

HOW TO HANDLE DATA AND NETWORK SECURITY RISKS EFFECTIVELY

There are three factors that help companies and individuals stay ahead of new and old threats and make sure they do not experience the consequences of a security breach: choosing the right endpoint security, device control and data loss prevention solution, educating their staff, and making sure their security experts are always aware of the newest threats and security solutions.

To make sure they choose the right endpoint security, device control and data loss prevention solution, company representatives need to consider how granular and effective control over portable device usage is, how strict file tracing and data access monitoring are, and if data in itself is protected when transferred through enforced encryption. Tracing the activity of users - what files they access or try to access when no allowed, what they copy where and which devices they plug in - is important to provide a comprehensive audit to the security staff and management and usually helps identify those with a malicious intent or those who would mistakenly try to introduce unauthorized devices in a protected network.

Granular policies are of great importance, as just blindly excluding everything is never the solution. Authorized portable devices are always needed, as the purpose of a good device control application is to allow companies to take advantage of all the business perks of new gadgets while staying safe. Restricting access to certain important company documents and making sure that sensitive information is always carried in an encrypted manner prevents the hassle of losing or exposing private details that could lead to lawsuits and costly settlements, fines or even losing the status of a reliable business partner.

Another key factor in properly dealing with the data and network threats of 2011 is to educate employees. While it may sound like quite an effort, the time a company and its staff invest in learning about the current threats and how to properly deal with them is of great value. Just think of the fact that when dealing with a data breach, the average US company spends about USD 500,000 just to notify the affected parties. While the costs are significantly lower in Europe, the average French company still spends about USD 120,000.

The key to making education easy and fun is using humor. The most successful educational campaign Endpoint Protector has run up to now consists of a series of comics published every week, depicting serious data breaches and how they happen in everyday business life. Training sessions don't have to be boring or don't have to be limited to gathering everyone in a room and having someone they will most probably ignore talk for an hour. Sending out an email blast with a fun drawing might prove a lot more effective.

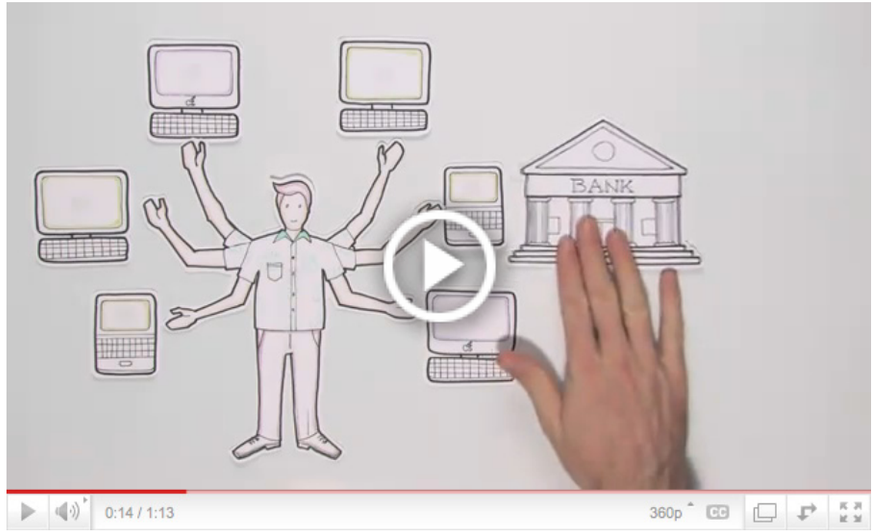
Education is an ongoing process. That is why security experts need to stay in touch with the industry, the data breach news and related fields to find out what they are dealing with and how to stop new threats. They will then be able to translate the information for the rest of the team that is not security-savvy and keep them updated about safe working scenarios.

ENDPOINT PROTECTOR DEVICE CONTROL AND DATA LOSS PREVENTION SOLUTIONS

Allowing companies to choose based on current needs, budgets and the staff they can rely on when it comes to company security, Endpoint Protector offers a varied range of security solutions that can easily integrate with existing infrastructures, are fast to learn and adapt to, highly flexible and extremely efficient.

ENDPOINT PROTECTOR HARDWARE APPLIANCE

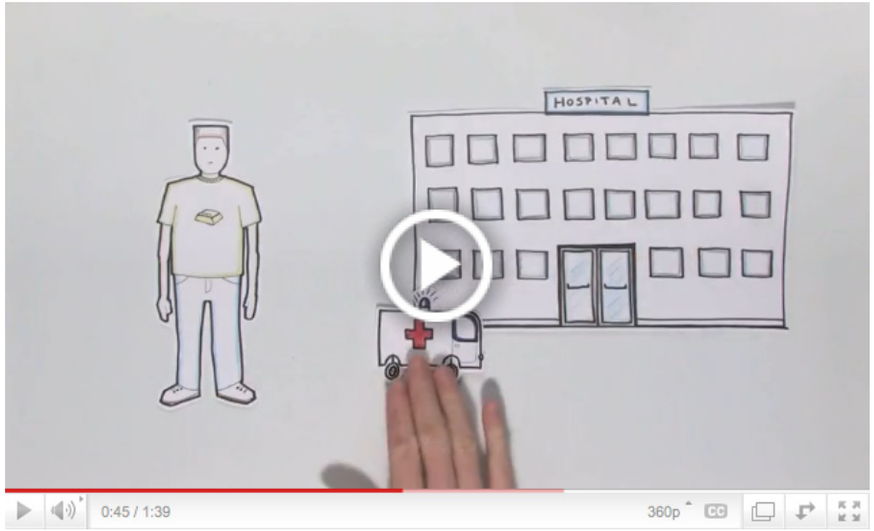
is a complete, ready to use solution providing device control and data loss protection in a fast and affordable way for both PCs and Macs in company networks. It allows companies to develop and implement a device security policy within minutes, while protecting existing resources and saving time and money.



ENDPOINT PROTECTOR
Working safe with portable devices

ENDPOINT PROTECTOR

is designed to minimize internal threats, reduce data leakage risks and control devices connected at Windows and Macintosh endpoints. It allows IT departments to proactively take control of the devices' internal use, while tracking all data transferred in or out of the protected network and enforcing encryption of data in transit on portable devices.



MY ENDPOINT PROTECTOR

makes enterprise-level device control and security accessible to even the smallest organizations without the need for expensive additional equipment or staff. My Endpoint Protector is an easy to manage, flexible and scalable security service. The total cost of ownership is significantly lower than conventional solutions - no purchase of hardware (servers, firewall, router, etc), no perpetual licensing model or annual maintenance fee.

REFERENCES AND FURTHER READING

Data theft record: 130 million card accounts stolen by Albert Gonzales - http://www.endpoint-security.info/2009/08/24/data-theft-record-130-million-card-accounts-stolen-by-albert-gonzales/

Data breach costs: TJX settles for 9.75 million dollars - http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1360065,00.html?track=NL-102&ad=711097&asrc=EM_NLN_8099563&uid=6425504#

TJX finds closure for breach in big time sale - http://www.theregister.co.uk/2009/01/23/tjx_sale/

Sensitive BP info revealed in hacking contest - http://www.endpoint-security.info/2010/07/31/sensitive-bp-info-revealed-in-hacking-contest/

Misplaced portable drive with 280,000 medical records - http://www.philly.com/inquirer/business/20101020_Health_insurers_say_data_on_280_000_Pennsylvania_clients_may_be_compromised.html

Lost thumb drive leads to potential data breach - http://abclocal.go.com/wpvi/story?section=news/local&id=7578794

Accomack county laptop stolen on employee's trip to Vegas - http://www.delmarvanow.com/article/20101014/NEWS01/101014035/1002/ACCOMACK--County-laptop-stolen-on-employee-s-trip-to-Vegas--residents--SSNs-compromised

7,000 CCNY Students Affected by Data Breach Exposing Sensitive Information - http://www.endpoint-security.info/2010/09/15/7000-ccny-students-affected-by-data-breach-exposing-sensitive-information/

Stuxnet and cyber warfare – the future is now - http://www.guardian.co.uk/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar

How to Stop Conficker/Stuxnet in four easy steps – Advisory by CoSoSys - http://www.endpoint-security.info/2010/09/28/conficker-stuxnet-cososys-advisory/

The Pentagon finally confirms the most significant breach of US military computers ever - http://www.nytimes.com/2010/08/26/technology/26cyber.html?_r=1&hp

US thumb drives finally allowed on Pentagon premises - http://www.endpoint-security.info/2010/02/28/pentagon-lifts-ban-usb-flash-drives/

Most employees would steal data. Companies worry, but do nothing - http://www.endpoint-security.info/2009/11/25/employees-would-still-data-companies-worry-but-do-nothing/

Europeans Protect Their Passwords, Not Personal Data - http://www.securityfocus.com/brief/725?ref=rss

The real cost of a security breach: 1 to 53 million USD per year - http://www.endpoint-security.info/2010/07/27/security-breach-costs/

Data breaches cost more in the US - http://www.endpoint-security.info/2010/04/29/data-breaches-cost-more-in-the-us/

Data Loss DB - Open Security Foundation - http://datalossdb.org/