The second in a series of eBooks on Cyber Security for business

CYBER SECURITY DEMYSTIFIED:

SECURING DATA

DATA: THE NEW OIL OR THE NEW ASBESTOS?

The amount of data generated by 2020 is expected to **jump by 4,300 percent over 11 years**.[2] But as the pace of data generation and usage increases, so does our dependency on it, both in business and in our day-to-day lives.

As the quantity and value of data grows, the pace of data breaches, **already up 57 percent over five years**[3], is bound to accelerate. After all, cybercrime and corporate espionage follow the money. That's hardly good for business. Data plays a bigger part in business processes than ever before. Its theft, corruption or deletion can threaten the viability of your business – or get you fired.

March 2014 was a turning point in cyber security. That's when C-suites around the world sat up and took notice. Target's CEO and CIO had both just resigned, in the aftermath of one of the largest data breaches in history.

The consequences of not taking data security seriously had become abundantly clear.

> "IT'S BEEN SAID TO ME THAT DATA IS THE NEW OIL, WHILE SOMEONE ELSE SAID IT'S ALSO THE NEW ASBESTOS."[1]
>
> - Sir Christopher Graham, UK Information Commissioner

DON'T FORGET THE CIA

The CIA Triad is a framework for information security: Confidentiality, Integrity and Availability. It's a model that can help you frame your needs based on the kind of data that you are securing and the controls that you have to deploy to achieve your goals.

C – CONFIDENTIALITY

Digital data is easy to steal: you only need to make a copy of it. To prevent sensitive information from falling into the wrong hands, you have to restrict access. The use case for doing so depends on the kind of data—from machine-to-machine communications to intellectual property. The trick is to ensure data confidentiality without making authorized access too difficult.

I – INTEGRITY

For you to be able to trust your information, data integrity must be assured over its entire lifecycle, while in transit and at rest. For example, if manufacturing parameters are manipulated, production equipment may not work. If the integrity of a voting system is compromised, the wrong candidate may win. Integrity ensures that data is neither intentionally nor unintentionally changed or deleted by unauthorized parties or events like a server crash.

A – AVAILABILITY

No matter how much valuable information you have, it's useless if it's not accessible. Lack of bandwidth may slow down a payment card transaction enough that customers simply takes their business elsewhere. Data availability is important to all businesses, but those with a need for high availability of sensitive data face a real security challenge.

DATA FOR SALE

Attackers are after all kinds of data. Even if they can't make use of it, they will attempt to sell it to those who can. Just days after stealing millions of U.S. military and government personnel records, hackers had login credentials up for sale on the Dark Web—a shadowy trading place for cyber attackers, illegal drug enthusiasts, arms traders and others.[4]

The kind of data that is of most interest to attackers includes:

PERSONAL INFORMATION

This includes banking details, addresses, social media logins and medical information, all of which can be used for frauds and scams of various types, including identity theft.

In the first wave of infection caused by the Heartbleed defect in 2014, a single U.S. hospital had 4.5 million patient records stolen. The data can be used to create fake IDs in order to buy medical equipment, drugs for resale, or to file bogus medical insurance claims.[5]

CREDIT CARD INFORMATION

Stolen credit card numbers are used to make purchases that are easy to convert to cash, like gift cards. They can sell for far less than USD $1 per record[6], payable in bitcoins on Dark Web sites accessed using a Tor browser.

Such browsers connect through multiple encrypted relays to obscure server location, masking the thieves' identity. One site offered 100 credit cards for $150, PayPal accounts at $100 for 100 and €1,250 in counterfeit bills for €500.[7]

DATA FOR SALE

TRADE SECRETS

Trade secrets, like financial data, pricing and sales details, upcoming mergers and other confidential business information can have devastating financial repercussions, should they be made public or fall into the wrong hands.

A recent survey pegs the cost of trade secret loss at between $749 billion and $2.2 trillion per year.[8] It's such an issue now that it has created political repercussions: in May 2014 the U.S. Department of Justice indicted Chinese military hackers on charges of infiltrating five large U.S. corporations and stealing trade secrets. Charges included aggravated identity theft, economic espionage and trade secret theft.[9]

INTELLECTUAL PROPERTY

For businesses that trade on their proprietary knowledge, methodology, process or formulations, IP data loss can spell corporate death or massively handicap competitiveness. In 2015, aerospace and defense sector respondents to a global survey reported a 97 percent increase in IP theft over the previous year—far higher than any other sector.[10]

THE COST OF TRADE SECRET LOSS IS BETWEEN $749 BILLION AND $2.2 TRILLION PER YEAR.

THE CONSEQUENCES OF DATA LOSS

Corporate data loss can hurt companies directly, but can also cause regulatory and legal headaches. Here are the top five consequences of data breaches:

LOSS OF STRATEGIC INFORMATION

Organizations can lose their competitive edge on activities when strategic inside information falls into the wrong hands. When hackers stole sensitive files regarding Coca-Cola's upcoming $2.4 billion acquisition of China Huiyuan Juice Group, the deal collapsed a few days later.[11]

BREAKING THE LAW

There are laws governing data security specific to many industries, notably healthcare. In the U.S., the Health Insurance Portability and Accountability Act (HIPAA) makes companies liable for the data they hold, with penalties of up to $50,000 per violation.[12]

COMPLIANCE VIOLATIONS

Data loss can trigger non-compliance resulting in serious financial repercussions. Merchants that accept credit cards, for example, must comply with the PCI Data Security Standard (PCI DSS) or risk losing their credit card processing privileges and fraud protection.[13]

LOSS OF LONG-TERM COMPETITIVENESS

When leaked data includes a secret formulation, a proprietary manufacturing process or ground-breaking research, businesses lose the kind of advantage that companies are built on. Algenol Biofuels has been able to guard its secrets for now, but loss of proprietary solar tech IP would have devastating consequences.[14]

LOSS OF CUSTOMER TRUST

When U.S. Target stores had customer credit card numbers stolen in 2014, customers stayed away and profits took a nosedive. A British telecom provider experienced the same kind of pain late in 2015 after they admitted a breach of over 150,000 customer accounts. The company has reported losses and costs topping £100 million .[15]

TARGETED...OR OPPORTUNISTIC?

Money is at the root of many data breaches.[16] Some of them, such as those involving theft of trade secrets, are the result of carefully planned, targeted attacks carried out by sophisticated corporate spies, criminal organizations or government-sponsored hackers.

The manufacturing sector accounts for more than 25 percent of all targeted attacks.[17] In July 2014 a Chinese national operating an aviation tech firm with offices in Canada was charged with hacking into U.S. aviation manufacturers Boeing and Lockheed Martin. Correspondence between hackers revealed his theft of 65GB of data from Boeing concerning its C-17, an advanced strategic transport aircraft.[18]

Most data breaches, however, are the result of opportunistic attacks that canvas the Internet, ready to exploit any vulnerabilities. These attacks are a numbers game that may reveal one vulnerability in 10,000. They are typically executed by means of a crimeware package, thousands of which are readily available on the Dark Web.

The criminals and organized crime syndicates that implement opportunistic attacks are typically not very sophisticated. They may be able to make use of credit card information, for example, but not social media profile logins. When they find data that they cannot exploit, they offer it for sale on the Dark Web.

THE MANUFACTURING SECTOR ACCOUNTS FOR MORE THAN 25 PERCENT OF ALL TARGETED ATTACKS.

THE ECONOMY OF DATA BREACHES

On any given day, an abundance of stolen data is available for sale on the Dark Web. For example, credit card numbers with PINs can sell for as little as USD $0.22, paid in bitcoins[19], although they can fetch $30 or more when they come with expiration date and full cardholder details.[20]

But while victims experience a loss that can typically be measured in dollars and cents, the profit for attackers depends on how well they can navigate criminal networks. Stealth, phishing and theft are very different skillsets from those required to monetize stolen information.

Some criminal organizations have vertically integrated the credit card fraud process, from data theft to final purchase. More often, card data is sold in bulk at a highly discounted rate. Dark Web buyers have almost no recourse if they are sold useless information, so trust is low. Card data is then resold in smaller batches, and at the end of the chain criminals create fake payment cards with real numbers and send individuals out to buy goods in-store that are easily resold.[21]

The advent of touchless payment cards puts a new twist on data theft. **A criminal need only read the information and copy it onto a blank card in order to make touchless purchases.**[22] Achieving a better understanding of the entire data theft/sales process as it evolves could ultimately help authorities to reduce instances of cyber crime.

> THE ADVENT OF TOUCHLESS PAYMENT CARDS PUTS A NEW TWIST ON DATA THEFT

THREATS FROM WITHIN

Current and former employees account for over half of insider leaks,[23] posing a clear and present danger when it comes to data loss. **Negligence and mistakes are common reasons for data leaks, but unhappy employees can leak data maliciously or take it with them to another company.**

In 2015, Coca-Cola reported a slow-motion data leak. Over the course of several years, an employee in charge of equipment disposal removed 55 laptops from the company's Atlanta offices. When Coca-Cola realized what had happened and recovered the laptops, they found that they contained 18,000 personal records and 56,000 records containing other types of sensitive data. None were encrypted in accordance with security policies.[24]

In a similar example, a hard drive containing sensitive information regarding 2,935 prisoners went missing from a British prison in May 2013. The UK Ministry of Justice had done the right thing in providing its prisons with encryption-enabled hard drives, but when the drive went missing in May, 2013 the Ministry learned that encryption protocols had not been followed, and in fact that encryption had never been turned on.[25]

Poor vendor security can cause just as much grave data loss. Finnish eLearning company Rockway narrowly escaped having its online business wiped out when its cloud-based streaming vendor closed its doors, and retail giant Target had millions of client records stolen when a heating and ventilation vendor's system was compromised.

CURRENT AND FORMER EMPLOYEES ACCOUNT FOR OVER HALF OF INSIDER LEAKS

WHO'S OUT TO GET YOU?

Data loss caused by employees or vendors is often accidental. With external parties, however, there is never any question about intent. Here are the usual suspects:

CYBER CRIMINALS

Cyber criminals can range from criminal organizations to lone wolves. They often specialize in one thing, like creating botnets. They may have specific targets, but will typically do anything that can be monetized. They offer their skills, the malware they produce, and the information they steal for sale on the Dark Web.

GOVERNMENT

Foreign governments target notably manufacturers, especially in the defense and energy sectors, as well as government agencies, as a way of gaining political or economic advantage. Hackers suspected of working on behalf of China recently infiltrated the U.S. Office of Personnel Management, stealing millions of U.S. military and intelligence officials' personal information.[27]

CORPORATIONS

Corporate spies carry out targeted attacks in order to steal competitors' IP. One survey unearthed a 64 percent jump in security incidents in Asia attributed to competitors between 2013 and 2014, likely government-backed.[26]

HACKTIVISTS

Hacktivists have a political agenda. They may wish to influence public perception on environmental or social issues, to change corporations' behaviour, like the hacktivist group Anonymous, or to impose an ideology at any cost, like ISIS. A recent phenomenon has seen hacktivist groups like Anonymous declare cyber war on ISIS and similar organizations in an attempt to cripple the Islamic militants' social networks.

110 MILLION CONSUMERS' DATA STOLEN

THE DATA THEFT

Fazio Mechanical, a third-party heating, ventilation and air conditioning (HVAC) contractor for Target Corp, was the source of the nationwide U.S. retail giant's data breach in late 2013. Fazio is suspected of intentionally being used as a stepping stone when its systems were infected by Citadel, a password-stealing bot program. Citadel enabled cyber attackers to gain access to one of three of Target's systems: an external billing system, a project management portal, or a property management portal. Once inside Target's network, attackers could gain complete access to all cash registers in every Target store, collecting credit card info and fooling AV detection. The information was transferred to a Target FTP server, which transmitted it to an outside virtual server in small batches.[28]

REPERCUSSIONS

Cyber attackers made off with a staggering 70 million credit and debit card numbers and 40 million shoppers' personal data. Some of that information is still being traded on the Dark Web. As a direct result of the scandal, Target's CEO and CIO both stepped down and the company was forced to fill these leadership positions.

Target has spent close to $100 million on breach-related expenses and new systems, and in the same financial quarter a year later profit was down 43 percent, or approximately half a billion dollars. Banks have taken action to sue Target as well, since the cost of replacing stolen cards alone reached $400 million. The cost in loss of customer trust, of course, is incalculable.

VENDOR CLOUDBURST

THE DATA DILEMMA

Rockway, a Finnish eLearning company, got a cryptic call from its cloud-based video streaming vendor just before Christmas. The vendor, which Rockway had been using for many years, called as a special courtesy to say that they could not, for an unspecified reason, guarantee service after New Year's Day in two weeks' time. As their business was fully reliant on the ability to stream videos, the company had to act fast to ensure business continuity.

To complicate matters, the only copies of the data were on the service provider's servers. In the end, Rockway staff had to hack their way through by creating a set of scripts that would download everything through the cloud vendor's APIs and reconstruct the data as a new database. Two weeks turned out to be just enough time to avoid business interruption, although the mere act of downloading the data took several days.

REPERCUSSIONS

In the end, Rockway managed to avert the crisis with no business interruption or loss. The company moved their data to Amazon, who at the time had just launched their video streaming service. The move was not without cost, however. They had to rebuild their entire online learning management panel, sync tools and other elements of their platform. On the bright side, Rockway learned its lessons and is now in complete control of its digital offering. They are in a position to transfer video streaming files to another host on short notice, if ever required.

32 MILLION CHEATERS EXPOSED

THE DATA THEFT

In August 2015, hackers calling themselves Impact Team accessed customer records at ashleymadison.com, the world's premier website for extramarital affairs. A month after the theft, the perpetrators published gigabytes of internal company emails, the login credentials of 32 million customers, and seven years' worth of credit card and transaction details, which bore customers' real names.[29]

In a Q&A with Vice.com's Motherboard magazine, Impact Team claims that they found "nothing to bypass—nobody was watching. No security. The only thing was a segmented network. You could use Pass1234 from the Internet to VPN to root on all servers."[30]

REPERCUSSIONS

Ashley Madison has been hit with more than $1 billion in lawsuits[31] from customers whose lives have been complicated by the breach in more ways than one: hackers are reportedly extorting money from site members by threatening to reveal their identity to friends and family.[32]

CALIFORNIA COMPANY CRYPTOLOCKED

THE DATA THREAT

Children in Film is a California-based company that acts as an advocate for young actors and their families. The company ran their operations—everything from Microsoft Office to QuickBooks—off an application hosting service at a managed cloud services firm.

Just before New Year's Eve, 2015, an employee opened an email attachment that looked like an invoice. Half an hour later, 4,000+ files, all stored in the Cloud, were locked to all employees. Every folder had a file that said 'help.decrypt,'—instructions on paying a ransom. The company's cloud vendor had been hacked.

THE SOLUTION

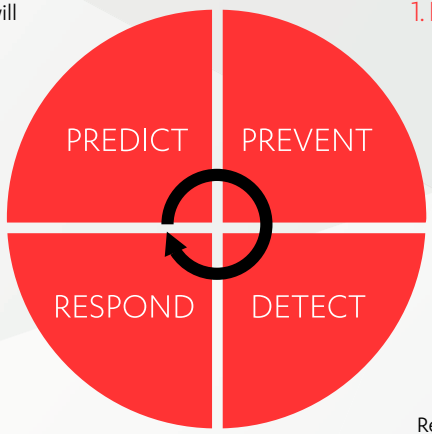
Children in Film's cloud provider kept daily backups, but it still took them almost a week to fully restore all of the files held hostage. The hosting service admitted that the malware also disrupted operations for other customers on the same server. Although the cloud provider had antivirus software installed, the ransomware was engineered to evade detection. Children in Film had never discussed the cloud provider's security setup when they engaged them, which is regrettable because obviously, cloud providers are vulnerable too. No hefty ransom was paid, but that is not always the case.

PREDICT, PREVENT, DETECT & RESPOND

When it comes to IT security, most organizations concentrate on locking the door. While keeping the bad guys out is an important goal, what if they get in? Guarding against more advanced attacks must assume that an incident will occur. A cyber breach can be contained and remediated quickly if your approach to IT security involves adaptive protection—a holistic process that integrates predictive, preventive, detective and responsive capabilities.

The key word here is 'process'. Our view of cyber security builds on concepts found in Gartner's Adaptive Security Architecture centered around risk management. If your business could be crippled by an IT security incident, you should adopt risk management processes for IT security, which turns resolution into a formal process.

On the following pages, we explore these steps as they pertain to data protection.



THERE ARE FOUR STEPS TO THE ADAPTIVE PROTECTION PROCESS:

1. PREDICT

Know your risks, understand your attack surface, and plan for the eventuality of both an attack and subsequent infection.

2. PREVENT

Minimize your attack surface and prevent incidents in the early stages of an attack.

3. DETECT

Recognize incidents and threats; isolate them and prevent them from spreading.

4. RESPOND

React to breaches, mitigate the damage, fix what's broken, ensure data integrity, and analyze post-attack.

DON'T BE A VICTIM

PREDICT

The smartest way to stay safe is to assume that, at some point, you will be attacked. Proactive planning will help you both contain a breach and remediate more quickly should one occur. Ideally, familiarize yourself with the kinds of attacks that affect your industry, map the most likely attack vectors, and set up business processes to limit data vulnerabilities. Pay close attention to the following regarding data security :

DATA MANAGEMENT

Data management is a good business practice with security implications. From a security perspective, it includes key planning steps like ensuring that data is in a secure location, identifying data critical to the survival of the business, who should have access to it, and evaluating what security measures are required, given its importance and risk profile.

CHOOSING A CLOUD VENDOR

With hosted storage or CRM systems, data security is handled entirely by your vendor, so consider them extensions of your own systems: put them under the same scrutiny as you do yourself. If you wouldn't locate your server in China, ensure that your vendors don't, either. Industry or legislative compliance requirements for your data will dictate where you can and can't locate it. Ask vendors to describe their security models and practices, recovery capabilities, physical access controls and restrictions. Find out who specifically will have access to your data, and what measures are in place to prevent social engineering attacks.

ANONYMIZATION

An important rule of thumb with data is to collect no more than you need, and to anonymize what you collect. Many Web service vendors, for example, unnecessarily collect users' home addresses. Take steps to separate your data, anonymizing it so that, for example, an address cannot be linked to a specific account. Also use hashing to ensure that you can use a non-human readable identifier. What you don't have you can't lose, and if you lose something that has been anonymized, it's less valuable.

DON'T BE A VICTIM

PREVENT

The following data security measures are designed to prevent access to data in usable form:

FRONTEND & BACKEND SEPARATION

The rule of thumb for utilizing public-facing servers or services is 'one system, one task'. Keep public interfaces and databases on separate machines. Compartmentalize them so that only predefined interactions are possible. For example, use a separate server for simple binary validation of passwords. That way, even if the public server is compromised, an attacker cannot obtain useful information from internal databases.

ACCESS CONTROL

A subset of data management, access control is a crucial part of compartmentalization. Clients should only be able to access the services and data that they require and users should only be able to access the network resources that they need. Depending on your business, physical access controls might be in order as well.[33]

NETWORK TRAFFIC ENCRYPTION

Virtual Private Networks (VPNs) are vital to ensuring data confidentiality when using public Wi-Fi or other untrusted networks. VPNs prevent traffic snooping, man-in-the-middle attacks, and also provide better authentication. Look for a reputable vendor, a strong encryption algorithm, and sufficient bandwidth.

FULL-DISK ENCRYPTION

Full-disk encryption renders databases unusable, ensuring data confidentiality in the event of device theft or loss, or the theft of a database. Full-disk encryption is increasingly required for legal and compliance reasons.

DATA HASHING

Data hashing is an important way of protecting passwords, notably with public-facing services. It protects passwords even if the password file itself is compromised, and also provides verification that a user's password is correct. Ensure that you use a proper password hash algorithm such as bcrypt, which is designed to prevent brute force attacks.[34] SHA-1 + Salting is not secure enough.

DETECT

Most companies focus on preventing intrusions, but don't have the capability to find and remediate them. When the end goal is preventing data exfiltration, detection is essential. If you don't know what happened (or is still happening), you can't contain it or rectify it. Detection serves three goals: finding out about ongoing attacks, finding previous attacks, and pinpointing an attack in order to isolate and contain it.

ACCESS LOGS/AUDIT TRAILS

One of the main ways to deal with suspected or actual cyber security incidents is through logging. Without logs it is not possible to determine what happened, who has gained data access, and by what means. Logs do many things, including providing proactive security: systems that recognize logged behavior can trigger alarms. To make logs relevant to your needs, they must be enhanced with proper sensor tools such as Sysmon.

NETWORK MONITORING

Basic network monitoring and traffic analysis is an important component of a complete intrusion detection solution. It can identify unauthorized access to services or data within a network, as well as gaps in perimeter defenses.

Above all, network monitoring should reveal source and destination IP addresses, as well as the data that travels between them. If your policy or business involves only local traffic, foreign access to your servers would be suspicious. Don't, however, neglect internal traffic: if you only look at network borders, you will miss internal host attacks.

HONEYPOTS

As the name indicates, honeypots are built to attract attackers. Fake database or other data storage locations trick attackers into accessing these dummy systems, alerting the IT team. Honeypots do two things: they distract attackers away from legitimate targets, and act as an early warning system. Most other alert systems generate a lot of false positives, but because no legitimate user should have access to a honeypot, the chances of an alert indicating a legitimate attack are extremely high.

RESPOND

After preventing or detecting and properly isolating an attack, the next step is remediation. When it comes to data, this involves resetting user passwords and access rights, ensuring data integrity, wiping lost or stolen devices, and restoring data from backups.

DATA INTEGRITY

The first step in remediation is to ensure that valuable data and systems have not been altered. This brings us back to the CIA model, specifically the 'I' for 'Integrity'. Data logs are an essential part of ensuring integrity. Compare your files and systems to previous integrity checks to identify additions, deletions or modifications of any kind.

DATA WIPE

To prevent data leaks caused by lost or stolen devices, you should have the capability of wiping the device in order to safeguard company information, even if the data would otherwise be unusable due to encryption, for example.

BACK UP & RESTORE

Robust data backup and restoration capabilities will allow you to recover more quickly and efficiently from security incidents. Restoring data safely requires clean backups, so it is important to first determine the duration of the incident, ideally with file integrity software.

To guarantee your ability to restore a system from backup, include the OS, application software and data in the overall backup procedure. Keep a backup virtual image of your production environment as well, in case you need to restore it quickly or change vendors. Be sure to keep any affected storage media or logs for forensic evidence.

Finally, don't forget to test backup procedures at regular intervals. Ensuring that everything works as intended, in addition to practicing backup restoration, will make the whole process more robust and efficient.

STEPPING UP SECURITY

March 2014 was a turning point in cyber security. That's when C-suites around the world sat up and took notice. Target's CEO and CIO had both just resigned, in the aftermath of one of the largest data breaches in history.

The consequences of not taking data security seriously had become abundantly clear.

Since then, hardly a month goes by without companies both large and small suffering public disgrace after losing their customer data. It is clear that doing the minimum is just not enough. Now is the last possible moment to start learning from other people's mistakes. The next one could be yours.

F-Secure provides security solutions for national defense and healthcare organizations, large manufacturers and other entities at high risk of attack. We know a thing or two about cyber security.

You can find our comprehensive cloud-based and on-site cyber security solutions for business here.

If your industry is more prone to targeted attacks for corporate espionage or other reasons, we can help. Get in touch to request an evaluation of your security environment, vulnerabilities or risks.

STAY SAFE OUT THERE.

> NOW IS THE LAST POSSIBLE MOMENT TO START LEARNING FROM OTHER PEOPLE'S MISTAKES. THE NEXT ONE COULD BE YOURS.

SOURCES

[1] Information Commissioner warns brands: customers will walk away over data breaches, campaignlive.co.uk, January, 2016 http://www.campaignlive.co.uk/article/information-commissioner-warns-brands-customers-will-walk-away-data-breaches/1381269#9wfwFjCQIAj1TB9e.99

[2] Big Data Universe Beginning to Explode, csc.com, 2012 http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode

[3] The History of Data Breaches, digitalguardian.com, September 2015 https://digitalguardian.com/blog/history-data-breaches

[4] Records from government data breach surface on 'darknet,' says expert, foxnews.com, June, 2015 http://www.foxnews.com/politics/2015/06/10/records-from-government-data-breach-surface-on-darknet-says-expert.html

[5] Your medical record is worth more to hackers than your credit card, reuters.com, September, 2014 http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

[6] Stolen Uber accounts worth more than stolen credit cards, cnbc.com, January, 2016 http://www.cnbc.com/2016/01/19/stolen-uber-accounts-worth-more-than-stolen-credit-cards.html

[7] Stolen credit card details available for £1 each online, October, 2015, theguardian.com http://www.theguardian.com/technology/2015/oct/30/stolen-credit-card-details-available-1-pound-each-online

[8] The Global State of Information Security® Survey 2015 - Managing cyber risks in an interconnected world, PwC, 2015 http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[9] Press release: U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, U.S. Department of Justice, May, 2014 https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[10] The Global State of Information Security® Survey 2015 - Managing cyber risks in an interconnected world, PwC, 2015 http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[11] Coke Gets Hacked and Doesn't Tell Anyone, bloomberg.com, November, 2012 http://www.bloomberg.com/news/articles/2012-11-04/coke-hacked-and-doesn-t-tell

[12] HIPAA Violations and Enforcement, American Medical Association. http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page?

[13] 7 Critical Consequences Of Failing PCI Compliance, Forbes.com, July, 2014 http://www.forbes.com/sites/sungardas/2014/07/01/7-critical-consequences-of-failing-pci-compliance/#6e0aa08263c2

[14] Cyber espionage: Small biofuel firm allegedly attacked 39 million times in 4 months, computerworld.com, July, 2014 http://www.computerworld.com/article/2476369/cybercrime-hacking/cyber-espionage--small-biofuel-firm-allegedly-attacked-39-million-times-in-4-mont.html

[15] TalkTalk admits losing £60m and 101,000 customers after THAT hack, February, 2016 http://www.theregister.co.uk/2016/02/02/talktalk_hack_cost_60m_lost_100k_customers/

[16] To Understand The Wave Of Breaches, Follow The Money, Forbes, February, 2013 http://www.forbes.com/sites/ciocentral/2013/02/01/to-understand-the-wave-of-breaches-follow-the-money/#658fdfdc7d6a

[17] The Global State of Information Security® Survey 2015 - Managing cyber risks in an interconnected world, PwC, 2015 http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[18] Chinese man charged with hack of Boeing, Lockheed Martin aircraft data, scmagazine.com, July, 2014 http://www.scmagazine.com/chinese-man-charged-with-hack-of-boeing-lockheed-martin-aircraft-data/article/360786/

[19] Stolen Uber accounts worth more than stolen credit cards, cnbc.com, January, 2016 http://www.cnbc.com/2016/01/19/stolen-uber-accounts-worth-more-than-stolen-credit-cards.html

[20] Here's how much your stolen data is worth on the Dark Web, bgr.com, November, 2015 http://bgr.com/2015/11/30/dark-web-stolen-data/

[21] The Underground Economy of Data Breaches, forbes.com, June, 2014 http://www.forbes.com/sites/frontline/2014/06/18/the-underground-economy-of-data-breaches/#688ac4e76c72

[22] Stolen Credit Card Details for Sale Online Calls Into Question RFID Technology, itbusinessnet.com, March, 2016 http://www.itbusinessnet.com/article/Stolen-Credit-Card-Details-for-Sale-Online-Calls-Into-Question-RFID-Technology-4321334

[23] The Global State of Information Security® Survey 2015 - Managing cyber risks in an interconnected world, PwC, 2015 http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[24] Coca-Cola suffers data breach after employee 'borrows' 55 laptops, techworld.com, January, 2014 http://www.techworld.com/news/security/coca-cola-suffers-data-breach-after-employee-borrows-55-laptops-3499054/

[25] ICO fines Ministry of Justice £180,000 for unencrypted data gaffe at 75 prisons, v3.co.uk, August 2014 http://www.v3.co.uk/v3-uk/news/2361825/ico-fines-ministry-of-justice-gbp180-000-for-unencrypted-data-gaffe-at-75-prisons

[26] The Global State of Information Security® Survey 2015 - Managing cyber risks in an interconnected world, PwC, 2015 http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

[27] Senior administration official: The latest China hack was classic espionage 'on a scale we've never seen before', uk.businessinsider.com, June 2015 http://uk.businessinsider.com/opm-hack-was-classic-espionage-on-a-scale-weve-never-seen-before-2015-6?r=US&IR=T

[28] Email Attack on Vendor Set Up Breach at Target, krebsonsecurity.com, February 2014 http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

[29] The Year's 11 biggest hacks, from Ashley Madison to OPM, wired.com, December, 2015 http://www.wired.com/2015/12/the-years-11-biggest-hacks-from-ashley-madison-to-opm/

[30] Ashley Madison Hackers Speak Out: 'Nobody Was Watching' motherboard.vice.com, August, 2015 http://motherboard.vice.com/read/ashley-madison-hackers-speak-out-nobody-was-watching

[31] 10 Things You Didn't Know About the Ashley Madison Scandal, alternet.org, September, 2015 http://www.alternet.org/sex-amp-relationships/10-things-you-didnt-know-about-ashley-madison-scandal

[32] Ashley Madison hack victims receive blackmail letters, December, 2015 http://www.bbc.com/news/technology-35101662

[33] Corporate Information Security – Network Security. Slideshare, Jarno Niemelä, F-Secure, 2014 http://www.slideshare.net/JarnoNiemela/network-security-29634400n p.47

[34] How Companies Can Beef Up Password Security, krebsonsecurity.com, June 2012 http://krebsonsecurity.com/2012/06/how-companies-can-beef-up-password-security/

[35] http://www.slideshare.net/JarnoNiemela/incident-response-29634418?qid=1473f355-d637-42cd-b059-a8234754c48b&v=qf1&b=&from_search=5

ABOUT F-SECURE

F-Secure has been solving business security challenges for over 25 years. We are a European pioneer in cyber security and data protection.

Our award-winning solutions go far beyond traditional anti-malware. We offer modern, best-in-class endpoint protection and vulnerability scanning tools in addition to security consultation. Developed in close cooperation with industry partners and international security authorities, our solutions garner global awards from leading independent experts.

Together with our network of over 200 operators and thousands of IT service partners, we are able serve millions of private and business customers locally, worldwide.

www.f-secure.com

F-Secure®