HANDD
BUSINESS SOLUTIONS

SECURING THE JOURNEY OF YOUR DATA

An advisory paper by HANDD Business Solutions

FOREWORD

The UK economy is transforming. Companies that used to rely entirely on paper are becoming digital natives, using sophisticated data tools to stay competitive. Analytics, the Internet of Things, and high-speed data networks are propelling UK businesses towards a bright future. Along with this comes an unprecedented threat: cybercrime. Today's crooks are as likely to break into your networks as they are into your physical premises.

Data protection issues are a rising concern for the public. The Information Commissioner's Office (ICO) received over 16,300 cases related to data protection in the 2015-16 year alone. It constantly tracks new technological developments and provides guidance on issues including encryption, safely removing personal information from data sets, and on small business cybersecurity.

More broadly, the UK government understands the extent of the problem but the onset of Brexit means that, along with EU relationships, the political landscape is changing. In late 2016, it committed £1.9bn to a five-year cybersecurity strategy that will include efforts to protect businesses and individuals.

The UK government has committed to helping businesses protect themselves from cybersecurity attacks, which threaten individuals, companies, and the entire economy. This is a joint effort, however; while the government is leading by example, businesses cannot rely on the public sector alone to protect them.

The government has published a ten-steps to cybersecurity guide[i], and recommends that companies create an information risk management regime across the organisation. Cybersecurity and data protection are cultural movements, rather than ad hoc projects.

Cybercriminals will continue to threaten UK businesses, but smart companies are already rising to the challenge. Thousands of them are already undergoing a digital transformation, preparing themselves for an information economy in which digital products and delivery mechanisms are changing the customer experience. Data protection is a key component in that journey.

Geoff Harris

Geoff is a CEO, a National Cyber Security Centre Certified Professional, former President of the Information Systems Security Association (ISSA)® UK Chapter and recognised international Cyber Security leader.

INTRODUCTION

HANDD
BUSINESS SOLUTIONS

Thirty years ago, cyberspace barely existed. Today, it is a battleground. Thousands of times each second, electronic crooks use it to probe company networks, testing for weaknesses. Looking for a way in.

Should they gain access, your data is under threat. The UK government's 2016 Cybersecurity Breaches Survey found that almost two thirds (65%) of large companies detected a cybersecurity attack in the past year, while 25% of them experience a breach at least once per month. The average cost was £6,500, but breaches that year cost up to £3 million, the report found[ii].

HANDD CEO and co-founder Ian Davin commented: ***"Companies must change their mindsets, looking at data not as a fungible commodity, but as a valuable asset. To criminals and customers alike, data is more valuable than gold. That puts your company in a challenging position as the steward of that data. C-Suite executives must understand the data protection challenges they face and implement a considered plan and methodical approach to protecting sensitive data."***

The need for a proactive business approach to cybersecurity is more intense than ever. Organisations must rise to the challenge. Slowly but surely, they are waking up to the problem, stimulated no doubt by mounting stories of compromised networks and stolen data. Even the most sophisticated organisations can fall foul of cyberattacks.

Despite its best efforts, one telco suffered the loss of nearly 157,000 customer records[iii], and thieves siphoned details from over 133,000 customer records at another[iv]. Financial institutions are also under attack, even though they diligently follow strict regulatory guidelines with their own compliance programs. Electronic intruders stole the personal bank details of almost 250,000 customers from one financial company[v].

An attacker only needs to succeed once, and these events show that even companies that focus on these issues can find them challenging.

As a board-level executive, you have a fiduciary duty to protect your customers' data. You already face up to £500,000 in fines if you fail, and under new rules, you will soon face millions more.

The situation is challenging, but far from bleak. A considered plan and a methodical approach to protecting sensitive data will put you ahead of the curve. Read on to find out how you can gain peace of mind – and a significant competitive advantage.

CHALLENGES

Before we explore solutions, C-suite executives must understand the data protection challenges that they face. There are a variety of factors, both technical and non-technical, that make effective data governance harder than ever. Some of those issues are discussed further here.

1 REGULATION

HANDD
BUSINESS SOLUTIONS

The General Data Protection Regulation (GDPR) replaces the 1995 Data Protection Directive, and comes into effect on May 25th 2018[vi]. It raises the privacy bar for EU companies including those in the UK, imposing extra data protection burdens on them.

Of particular significance here are the penalties involved. Companies violating the new rules face penalties of either €20 million, or 4% of their global revenues, whichever is higher. This escalates existing penalty options for national data privacy authorities, including the Information Commissioner's Office in the UK. Organisations cannot afford to ignore these new rules, and must review the data protection procedures to ensure compliance.

It is also worth noting that GDPR is not a 'set it and forget it' project. The rules specifically call for companies to assign responsibility for privacy and data security to someone in the organisation, and to monitor and measure privacy and security practices on an ongoing basis.

CASE STUDY

Handling Compliance, European Bank:

When financial institutions don't adhere to compliance regulations, they face major problems. A large European bank experienced this first hand, after failing a security audit. Auditors had identified problems with the way the bank managed its SSH keys. The bank didn't know which devices had which privileges so potentially, anyone using these devices could gain access to any of its internal resources. HANDD began with a full audit of the SSH estate. The results were worrying, 23% of the SSH keys were more than 5 years old, 68% had no IP restrictions and 90% of the access permissions were obsolete. HANDD remediated the problem by revoking the obsolete and insecure keys. Then by developing a process for the ongoing management of certificates the bank dramatically reduced its security risk and passed their next audit.

2 MANAGING ACCESS TO DATA

One of the biggest challenges for companies trying to protect customer data is controlling who has access to it. This is a nuanced issue, because proper access management dictates that users must have different privileges within the system depending on their roles and responsibilities. Least-privilege access ensures that a junior account manager only sees the data they need to, and can only manipulate accordingly.

Privilege management involves subtleties that many security teams do not spot, including temporary privilege escalation. Accounts with permanently-elevated privileges are vulnerable in several ways. An attacker could steal access credentials and use the account to wreak havoc at the organisation, or a legitimate insider could inadvertently misuse the account.

For example, a user with an account capable of running executables could mistakenly run a malicious file and compromise the entire network.

Companies can mitigate this threat by requiring users to manually elevate account privileges, and logging the event. For even more protection, a secondary administrator could be required to check the request and grant access. Smart companies will use tools that record video of user sessions. This can be a useful way to audit sessions that use ad hoc privilege escalation.

Not managing data access properly can lead to insider threats. Malicious employees may steal sensitive data for personal gain or for ideological reasons. Some users with the best of intentions may still put the company in danger by sharing information that they shouldn't.

3 EDUCATION & AWARENESS

HANDD
BUSINESS SOLUTIONS

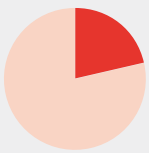
Raising end-user awareness and improving security consciousness is another challenging area for companies. User awareness programs are important for organisations that want to introduce a culture of security, and organisations must give them the attention they deserve. Effective user awareness initiatives are not one-off initiatives. After explaining cybersecurity principles to employees and getting them to buy into the concept, an effective program will measure employee awareness on an ongoing basis and reinforce it over time.

Companies can take advantage of third party expertise in cybersecurity training. An adept partner will help them to drive cybersecurity awareness into a company's culture.

Both access management and training extends to anyone with access to company data. This often goes beyond employees to contractors and external partners, extending the management challenge.

Smaller Firms Can Do More To Train Their Staff

Businesses where staff have had cyber security training in the past 12 months:



Small: 22%

Medium: 38%

Large: 62%

Source: Government Cyber Security Breaches Survey 2016. Professor Mark Button and Dr Victoria Wang.

4 SKILL & RESOURCE

There is a serious cyber security skills shortage in the UK with the gap between supply and demand for expertise increasing at an alarming rate. Currently, there are three times[viii] as many IT jobs out there as there are available candidates. Equally, a recent report[ix] suggests that there could be as many as 1.5 million security jobs to fill by 2020. HANDD have seen a rise in the number of organisations approaching us for our expertise and resource in this area.

5 EMPLOYEE PUSHBACK

Pushing through security policies is not simply a case of introducing new technologies. Sometimes, organisational structure gets in the way. Different employees and business units can have competing agendas, and these can conflict with each other. In some cases, a desire to simply 'get the job done' can hinder otherwise sound security principles.

A business unit that owns an application or data set may not take kindly to a security team putting access barriers in front of it, for example. If employees believe that it disrupts working patterns and hinders productivity, it can create political blowback within the organisation. This is why helping employees to understand the need for cybersecurity and making it part of a company's culture is such an empowering process.

CHALLENGING TECHNOLOGY DEVELOPMENTS

Organisational issues are not the only challenges facing companies that need to protect their data more effectively. Technology innovation marches on, and each development presents new security problems for those charged with keeping data safe.

1 BYOD (BRING YOUR OWN DEVICE)

Mobility is a perfect example of how organisational and technical issues affect each other. Users are increasingly bringing their own devices into work. This creates a risk of data theft through lost/stolen devices, or through malware infection on unmanaged kit. Some users, especially senior executives, may be unwilling to relinquish their smart phones, tablets, or hybrid devices even though they represent a potential security weakness. This creates a mixture of technical and political issues for IT departments, which must balance two objectives: safeguarding data and being responsive to users.

Just as employees may want their own devices, they may also want their own cloud services. Those who use cloud services that your IT department has not authorised can create a black hole for your data.

2 BIG DATA

Another technical challenge is the rising tide of data. Data is increasing in volume and velocity, especially with the evolution of big data/analytics. In fact 90% of the data in the world today has been created in the last two years alone, at a rate of 2.5 quintillion bytes of data per day.[x] Unstructured data ranging from Office documents to social media posts co-exists with the tabular records in company databases. There is more of it each year, and managing it manually becomes increasingly difficult.

Each piece of data has its own level of sensitivity, its own compliance requirements, its own sender and recipient. Some data may seem innocuous on its own, but could be a privacy time bomb when paired with other data housed in enterprise systems.

3 CLOUD v ON PREMISE

Cloud provides tangible benefits: cost management, resource elasticity, and a lower skills overhead. But it also offloads data to a third-party resource. You must manage cloud security just like any other part of your infrastructure. While it is possible to create a secure cloud computing environment, it isn't guaranteed.

Companies must define the cloud service provider's responsibilities along with their own, and must then ensure that their own policies can be adequately supported in a cloud environment. More than two thirds of companies (67.8%) note that an inability to enforce corporate security policies is an obstacle to cloud adoption[vii].

4 IoT

The Internet of Things (IoT) may not feature in a company's long-term strategy, but that doesn't mean it can be ignored. Connected devices filled with sensors are coming to all market sectors from utilities and health to financial services and local government. Some of them may arrive in the form of sanctioned purchases like smart TVs for the boardroom, while employees may bring others without thinking to ask permission.

All of these connected devices serve as an extra attack vector once on corporate networks. Attackers may be able to glean useful information from the devices themselves or alternatively, they can use a compromised IoT device as a launch pad to attack other devices on the network.

YOUR DATA'S JOURNEY

Companies dealing with these threats need a cohesive approach to data management that involves four things: people, process, policy and technology. Software and hardware tools are a crucial part of protecting information in a digital environment, but they alone won't solve a company's cybersecurity problems. It takes a well thought-out data management workflow to eliminate security weak spots, and a properly-trained workforce to enforce it.

Data should have a lifecycle in an organisation; a structured journey that enables administrators to constantly manage it. Companies should be able to monitor and measure their data security practices on an ongoing basis, as this is a specific requirement under the GDPR.

Effective data lifecycle management calls for a mixture of policy and technology that many companies have not yet created, making it difficult to control or manage their data in any meaningful way. Here is what the four stages of the data journey should look like when a company is protecting its information.

YOUR DATA'S JOURNEY

> "Many organisations have no insight into the data that they hold and so don't understand which data is worth heavy investment. The reality is that they could be spending as much on securing the lunch menu as they are on securing their customers' data"
>
> **Danny Maher, CTO at HANDD**

1. Creation

Data enters an organisation in diverse ways. A company may gather it from a customer when taking an order via a web site or over the phone. A customer may add it via an online app, or it may be acquired from a data broker. A business partner may provide it, or it may be acquired during a merger. Each data item will have its own characteristics, such as its sensitivity level and its longevity.

Analysing and documenting these characteristics is a vital part of a data item's journey throughout an organisation. Without proper classification, managers cannot make informed policy decisions about the information that they're collecting, which opens them to security and regulatory risk.

Metadata is the solution to these problems. When data is created, a comprehensive data lifecycle management and protection solution will classify it by 'marking' it with digital tags that describe its characteristics. The classification system will tag data items or documents with markers defining useful attributes, such as a sensitivity level or a retention requirement. This then helps data management systems organise the data in compliance with company policy.

Tagging new data isn't enough. To be truly effective, a classification system will apply tags to existing data, too. Most companies will already have

YOUR DATA'S JOURNEY

gigabytes or more of data that they created before introducing such a system. The data management system must find that legacy data, which will be distributed across many different endpoint and server computers within an organisation.

2. Storage

When a company creates data, it must then store it. Should it be stored in the cloud, or on the company's own premises? If a company stores data in-house, should it be on a public server, accessible to all employees, or on a private one, accessible on a need-to-know basis? Should it be instantly available, or archived on cheap, slow-retrieval media? Recent research carried out by HANDD revealed that 35 per cent of IT professionals cited ensuring data is stored securely, and whether it's on premise or in the cloud, as their biggest challenge and most likely to keep them awake at night.*

A data record's classification should enable a company to make these decisions, automatically and definitively dictate its location. It should also enable a company to decide which encryption policy it will apply to that data.

Some records will be so sensitive that their owners should encrypt them wherever they are stored. If companies use a safe encryption algorithm, the act of encryption is not a complex task. However, managing the encryption keys that grant access to that data is a demanding process that requires an understanding of access privileges and digital certificate management. This isn't something that many companies will want to manage securely themselves.

3. Data Access

Once a company has stored data in compliance with its security policy, data management systems must then stick to those policies when granting access to that information. Only the users that need information should be able to see it, which means that an access management system must understand their roles and responsibilities.

Identity and access management (IAM) is a powerful tool when building secure access mechanisms. It manages users' logins, ensuring that only those people with the right credentials can get in. Modern access systems should be using two-factor authentication to make security more robust. This uses not only something you know (your password) but also something you have (such as a hardware token or a mobile phone), making it far more difficult for imposters to compromise a user's account.

An IAM system will use the concept of least privilege, classifying users according to their roles and giving them access only to the data they need. An IAM system might only give a junior sales executive access to the names and numbers of customers to

** Full survey results on inside back cover*

which she has been assigned, while granting the VP of sales access to the entire database.

What if the VP of sales proves to be dishonest, and wants to sell that customer information to a third party? Another tool, user behaviour analytics (UBA), comes in useful here. It alerts managers to unusual activity that falls outside a person's regular behaviour patterns. If an employee who only accesses company records from a single PC during office hours suddenly tries to download files from another device outside the organisation in the middle of the night, a UBA tool will notice.

Increasingly, these tools are using another key technology to help them spot more anomalies: machine learning. This is a form of artificial intelligence that mines historical data to look for patterns, establishing a baseline of normal behaviour.

Used correctly, machine learning can help security administrators to find a needle in a haystack. As modern computing infrastructures generate increasing amounts of data, human operators find it hard to spot potentially dangerous incidents amid a rising tide of system events. Artificial intelligence provides an automated layer that can surface appropriate events and help them focus their attention where it is needed.

By using machine learning to analyse employees' past data access patterns, IAM and UBA systems can then measure all future behaviour against an acceptable norm, and raise the alarm if something seems amiss.

4. Sharing & Collaboration

Security doesn't just stop at who accesses your data; who they share it with, how long for and via what medium is a key consideration too. Thanks to the metadata tags that you created along with the data, your systems can use predefined policies to make those decisions on a per-document basis. This concept, known as information rights management (IRM), is a powerful data protection mechanism.

IRM isn't going to save you if you share your files via email. Email is an insecure mechanism that often sends data – including your sensitive files – in plain text. Instead, use Managed File Transfer (MFT).

MFT is like Dropbox, but with a robust security framework that puts the user in control. It manages the transfer of your files from end to end, providing secure encryption, non-repudiation (you can prove that a file was sent and received), and automation. IT teams can also produce reports for business users to show which files were transferred, and when.

YOUR DATA'S JOURNEY

The other complementary technology is data leak prevention (DLP). This technology alone will not prevent malicious users from transferring sensitive files outside a company, but it is a useful way to stop unwitting users from accidentally sending sensitive data. DLP looks for data in a certain format (such as customer names and addresses, credit card numbers and social insurance numbers), and blocks them from leaving the company.

5. Archiving or Removal

All data has a lifecycle often dictated by regulation. Some industries require companies to keep data for a certain time, and some regulations require sensitive data to be deleted when no longer needed. As data volumes increase, managing these records becomes burdensome. Here, again, metadata comes to the rescue. Combining tagged files and automation enables you to set policies around your data disposal and archiving, ensuring that zombie data isn't creating an unnecessary security risk.

CASE STUDY

Safeguarding File Transfer, NHS Wales: NHS Wales, who have 65,000 staff nationwide were faced with a problem of being able to send information securely around it's many sites.

Due to strict regulations, they needed to protect patient privacy whilst sharing large and highly sensitive files. Ultimately, they wanted to simplify and regulate the flow of information between its Trusts. NHS Wales approached HANDD for a solution. This process started with a consultation service to understand the requirements, followed by HANDD's design, implementation and support services to deploy a managed file transfer solution.

The new managed file transfer solution enables NHS Wales to exchange sensitive information swiftly, securely and fully audited.

HANDD'S APPROACH

The steps involved in data protection are complex and demanding, both from a technical perspective and a business one. Companies that don't specialise in these processes will find it difficult to cover all the bases on their own. HANDD can help you structure your data's journey and protect it along the way, using a comprehensive four-step process:

Securing The Journey of Your Data

ANALYSE

When protecting your business against any threat it is vital to have a full understanding of your people, policies, processes and data. HANDD consultants identify vulnerabilities and mitigate risk.

PROTECT

Protecting your data begins from the moment that it is created. HANDD will work with your organisation to help you to protect your data throughout its entire journey.

DETECT

Data is vulnerable to attacks from both internal and external threats. HANDD provides real business intelligence to give you full visibility and control of your people, processes and data.

RESPOND

It is no longer a case of "if" but "when" an attack will occur. HANDD will help your organisation respond, recover and restore normal working practice in the event of an attack.

Contact us today to take your first step.
Visit www.handd.co.uk or call +44 (0)8456 434 063

SUMMARY

Data protection is a daunting prospect for companies, and the threats are only getting worse as attackers develop more innovative methods of defrauding your company. No one product or technique will prevent these exploits, because cybercriminals use a variety of tools and tricks to get at your sensitive data. A truly sophisticated cybersecurity solution uses a multi-layered approach to detect and prevent a variety of attacks, and includes contingencies for dealing with intrusions when they do occur. It also includes an ongoing monitoring and measuring of existing security practices to ensure that companies stay on track and keep protecting their sensitive data, even as the business changes.

Working with a cybersecurity solutions provider to protect your data – and your customers' data – from end to end gives you a distinct business advantage. Not only does it buy you compliance with increasingly strict Europe-wide regulations, but it also gives your customers peace of mind. As the data breach headlines mount and household brands repeatedly face embarrassment in the press over lost data, customers are looking for reassurance that product and service providers have taken the time to protect their interests.

Get ahead of the game.

Protect your information assets now.

Rereferences

[i] https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
[ii] https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016
[iii] https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack
[iv] https://techcrunch.com/2016/11/18/three-uk-suffers-major-data-breach-via-compromised-employee-login/
[v] http://www.bbc.com/news/business-39544762
[vi] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[viii] https://downloads.cloudsecurityalliance.org/assets/partners/CSA_Skyhigh_Survey_-_Cloud_Balancing_Act_01-16.pdf
[viii] http://www.independent.co.uk/news/business/news/cyber-security-skills-gap-widen-supply-demand-expertise-uk-companies-it-a7529986.html
[ix] http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html
[x] https://www.mediapost.com/publications/article/291358/90-of-todays-data-created-in-two-years.html

In June 2017, HANDD commissioned a survey of 300 IT professionals in the UK.

HANDD
BUSINESS SOLUTIONS

HANDD Survey Results

21%

of IT professionals say **regulations, legislation and compliance** will be one of the biggest challenges to impact data security.

41%

of those surveyed assign the **same level of security resources AND spend for ALL company data,** regardless of its importance.

35%

say **ensuring data is stored securely**, and whether it's on the premise or in the cloud as their **biggest challenge and most likely to keep them awake at night**.

41%

say employees are an organisation's **greatest asset.**

21% believe that the behaviour of employees and their reactions to social engineering attacks poses a big challenge to data security.

45%

of IT professionals are confident they **have an Identity Access Management process** in place that dictates that users must have different privileges depending on their roles and responsibilities.

Worryingly, 15% have absolutely no Identity Access Management process in place.

HANDD
BUSINESS SOLUTIONS

SECURING THE JOURNEY OF YOUR DATA

HANDD Business Solutions (HANDD) is an independent specialist in global data security. They work with some of the leading vendors in the data security market. Established 10 years ago, their goal is to provide customers with industry-leading solutions that analyse and protect data through every aspect of its journey.

HANDD has more than 500 clients spanning 25 countries across the energy, financial services, insurance, manufacturing, retail and utilities sectors. These comprise 45% of the FTSE 100, eight of the world's largest banks as well as a host of global organisations.

Following its carefully developed four-step strategy of analyse, protect, detect and respond, HANDD's specialist knowledge and unrivalled expertise makes it a trusted advisor in securing a client's data wherever it travels, from consultancy and technical design, through to implementation, training and support.

www.handd.co.uk
info@handd.co.uk
+44 (0)8456 434 063