Guernsey Financial
Services Commission

Industry Seminar – 20 October 2011

Data Security Presentation

Donal Kennedy – Assistant Director, Finance and Operations Division

Thank you and good afternoon.

For those of you who don't already know me, my name is Donal Kennedy and I am an Assistant Director in the Finance and Operations Division.

My primary role is the management and development of the Commission's communications and information systems. This covers both daily operational performance and data security.

Before I start on Data Security, let me quickly remind you why I'm presenting in this specific session for Fiduciary Division.

At the outset it's important to recognise the diversity in size of the Fiduciary sector licensees. The range is greater than in any other Division. Your businesses vary from personal licensees up to large organisations

Smaller organisations are generally more vulnerable. Protection systems are not as sophisticated. There is less understanding of the technical measures necessary.

The trend from data breaches investigated worldwide is that smaller organisations are now more targeted.

The barriers, and the risk of detection are typically much less.

Schedule 1 of the Fiduciaries Law covers the Minimum Criteria for Licensing. Paragraph 1 states that a licensed fiduciary will operate with prudence and integrity and in a manner that will not tend to bring the Bailiwick into disrepute as an international finance centre.

Paragraph 5 further defines prudence and states that we will consider your systems of control when determining whether you conduct your business in a prudent manner.

Data Security is just one of the many systems of control that every fiduciary licensee must address.

I will talk today about the importance of data security, and some of the key areas we must all address, and also about the Commission's Extranet project.

There is no "one size fits all" solution to data security.

However, we all have a responsibility for Data Security, regardless of seniority, or indeed what size of organisation we work for. Let’s start with the importance of Data Security.

Data Security should be based on a risk assessment. It should be management’s decision.

It needs to take into account all threats and hazards, whether they arise from cyber-attacks, or natural disasters, or indeed any other source.

The Verizon business risk team produces an annual review of the security breaches that both they and the US Secret Service investigate.

In their 2011 report released earlier this year there are many frightening statistics, but two stand out:

Firstly, 96% of the breaches investigated could have been avoided with basic and relatively inexpensive security controls.

And secondly, there is a visible trend of a huge increase in smaller external attacks as small to medium-sized businesses represent easier attack targets for many hackers.

The report is freely available on their website.

Data breaches can cause harm and distress for those affected. They can lead to serious financial losses and they can seriously affect reputations.

For example, in late 2008 and early 2009, Manchester City Council suffered an extensive virus infection on their network. It was thought to have come from a virus infected USB memory stick.

It cost them £1.5m to put right.

We are all the custodians of other peoples’ data and we must earn and retain their trust and confidence. In the Commission, we are governed by Section 21 of the Commission Law which makes confidential all licensee data that we receive. As fiduciaries, you too have a duty of confidentiality to uphold. Actions regarding Data Security are a key part of that duty.

A key principle of the Data Protection Law is that those processing personal data must have adequate security precautions in place to prevent the loss, destruction or unauthorised disclosure of the data.

Guernsey’s Data Protection Commissioner has issued clear guidance to Financial institutions including the requirements for security under the Data Protection Law.

Copies are available from the Data Protection Office or on the Data Protection website.

In the UK, the FSA has fined one firm in excess of £3m for failing to adequately protect customers' confidential details from being lost or stolen.

We must recognise that a data loss by any of us, no matter what size our business is, will not only affect our own reputation, but also that of Guernsey plc.

In summary, the importance of Guernsey's reputation as an international finance centre means that Data Security must be addressed by everyone!

We're now going to look at key areas of focus, which I have categorised into three main areas – Strategy, Technology and People.

Let's briefly take a look at each in more detail.

In terms of Strategy and Documentation an initial risk assessment needs to be undertaken to review what measures are appropriate to the specific business.

Responsibilities must be clearly defined so that there is complete clarity on who is responsible for safeguarding the data.

There needs to be appropriate policies and procedures and contracts with third parties.

For Technology Measures, we need to identify and implement essential controls. We need to ensure their implementation across the organization without exception.

Practical Examples include:

- Keeping PC and Server applications and operating systems patched and up to date including monitoring for new patches on a regular basis
- Encrypting portable data in its many forms including laptops, USB keys, CDs and Backup Tapes
- Changing default credentials and ensuring that passwords are unique and not shared
- Regularly reviewing user accounts. Confirm that active accounts are valid & necessary
- Monitor network and firewall logs. Often, evidence of "events leading to a breach" already existed in logs prior to the actual breach
- Give appropriate access to systems. Don't give users more privileges than they need - Trust but verify that that trust is valid.

To address people aspects of data security, there must be a focus on people's behaviours. We need to ensure that policies and procedures are complied with.

People are rightly considered the weakest link in data security. They are generally resistant to culture changes, therefore this element, more than most, must be led from the top.

Training and awareness programmes also need to be set up.

For those of you that want to go back to basics, I suggest Business Link. This is the UK government's free online resource for businesses.

It contains essential information including data security for any size of business.

Also listed are the local Data Protection Site and the Verizon security blogging site.

The Australian Defence Signals Directorate also conducts an annual breach survey with recommendations.

From a technical viewpoint, they maintain a list of 35 prioritised strategies to mitigate against cyber intrusions, even detailing the likely resistance you will face from your users should you try to implement each one.

It is interesting to note that they have confirmed that addressing their top 4 strategies would have prevented 85% of the breaches they investigated in 2010.

The top three should be standard in most businesses already:

- Patching both applications and operating systems but within two days for high risk vulnerabilities
- Minimise the number of users with domain or local administrative privileges. Such users should also use a separate unprivileged account for email and web browsing.

The fourth strategy is less common, but important nonetheless:

- Application whitelisting helps prevent malicious software and other unapproved programs from running. *e.g. by using Microsoft Software Restriction Policies or AppLocker.*

Overall, it is worth reviewing your security arrangements to see how you compare to best practice, but don’t forget the non-technical measures I’ve detailed today.

The last of my agenda items is focused on what we are calling our Extranet project.

It concerns the automated processing of licensee information and risk assessments. It will address our security concerns on the transmission and storage of your sensitive and confidential data.

In implementing systems and process enhancements to provide for this automated processing, we could both benefit in a variety of ways.

We can both achieve efficiency enhancements from the automation of manual processes. For the Commission that will include eliminating the re-keying of data and the scanning and archive of paper-based documents. It will enable us to re-focus our efforts on more value-added activities.

For licensees, it may include more automated production of your submissions.

For both of our benefits, we will look to automatically validate submissions. This will eliminate inefficient correspondence.

Once licensee information has been submitted we intend to automate, where possible, our standard analyses so that the initial automated assessments of submissions can assist us in targeting our work efforts.

In terms of data security, one of the key objectives of the system is to provide a secure communications channel between the Commission and external third parties, such as licensees.

Overall data quality within the Commission’s internal systems, will be enhanced by eliminating the re-keying of data.

The automation of our initial analyses will reduce the risk that we don’t act on information received in a timely manner. This is particularly relevant where we receive large volumes of data at the same time. E.g. Large volumes of returns are received in April, being 4 months after December year ends.

And finally, electronic records are backed up and available in both our main and recovery locations, thereby improving business continuity.

We need your input on the scope of the project.

We have already been liaising with industry bodies across all sectors and if you have any suggestions or want to get involved on the project, would you please contact your industry body in the first instance. Alternatively both Fiona Crocker and I are also contactable at the Commission. Submissions have been requested by the end of November at latest.

The current slide shows a small selection of important data which may be included, but the list is by no means exhaustive. What is also important is the inherent functionality that is required in the system. For example, how an approval process would work if required and what impact that would have on you. What methods of submission you would expect – Forms based and excel based are likely, but does anyone require bulk data transfers to us?

We can also learn from your experiences in providing similar systems to your clients.

The selection of the scope for the initial project will focus on achieving essential requirements.

In defining the scope of the first phase, we will use a risk based approach, whilst also considering costs against benefits.

The indicative timeline is that we expect the system to go live in 2013.

The threats against our data are real. They are constantly evolving and will continue to pose a serious risk to our businesses. They come from a variety of sources including individuals acting alone, issue-motivated groups, and not surprisingly from criminal elements.

We all need to be proactive to protect our data. It is not possible to prevent all breaches.

Therefore we must also develop plans for how to respond should our data be compromised.

Today, we've briefly covered the importance of Data Security, and some statistics on data breaches.

We've looked at some of the measures that we should all have in place, and I've provided you with additional online resources for later review.

And finally we've looked at our Extranet project and how we intend to improve the security of the data we receive from licensees.

Finally, if you only take three words from my presentation, try these: Responsibility, Protection and Reputation.

We all have a responsibility for Data Security;

We must take proactive steps to protect our data; &

The Reputation of Guernsey plc is at risk if we don't address our individual responsibilities.

Thank you for listening, and I shall now hand back to Philip for his closing address.