ISACA®
Serving IT Governance Professionals
Scottish Chapter

Newsletter - April 2009

This is the second all-electronic newsletter and, hopefully, members are finding this format accessible. The Chapter is working on other ways to allow members to access the content: keep a look-out for a podcast version, which will be ideal for the drive to work.

In this newsletter, we look at the lessons that can be learned from airline crashes, spend some time "using our imagination" and - since it's impossible to ignore the wider financial situation - identify how you might approach audit in the downturn. We also have the latest installment from Lucy Adam on getting your ideal job. Whether you've experienced plenty of interviews, or have been in your current situation for a while, there are a lot of valuable tips to help you brush up your technique when pitching for the dream role.

As noted in "News in Brief", ISACA is now 40 years old. While the Scottish Chapter is a relatively recent part of the story, it's reassuring to know that the efforts of tens of thousands of professionals have helped build on the early days of the EDP Auditors Association. A brief presentation on our history can be found on the ISACA website and is well worth a few minutes of your time.

Finally, the membership roll for the Chapter will be "purged" during April, to remove anyone who has not renewed their ISACA membership. Being a member of ISACA allows you to actively join in with and contribute to the development of the global profession, as well as benefitting personally through the wide range of resources on the ISACA website. You can also gain from the local activities of your Chapter - including this newsletter - and a range of free or heavily-discounted training events to maintain those all-important CPEs. You can quickly sort things out by logging in to the ISACA website and clicking on "My Renewals".

...news in brief...

ISACA marks its 40th anniversary in 2009

...news in brief...

Survey of over 2,600 companies worldwide reports that 68% are underspending on IT security relative to the financial losses they are incurring - almost 10% revenue in data loss and theft alone

...news in brief...

The Peruvian government has recognised the CISA certification, and notes that systems auditors will use ISACA IS Auditing Guidelines

...news in brief...

The IIA proposes a new Postgraduate Certificate in IT Auditing for existing PIIA, MIIA and CIA holders, to be measured through an exam and a project

...news in brief...

The IT Governance Institute offers a white paper on the adoption of ISO/IEC38500:2008, the new global standard on IT corporate governance

...news in brief...

ISACA updates ten IT audit programmes, including change management, identity management, IT continuity planning, outsourced IT environments, security incident management and Unix/Linux security

...news in brief...

Contents

Presidential Cogitations

Tony Povoas

The current economic recession and commentary surrounding it appear ubiquitous. Writing a column for the ISACA newsletter, without considering the impact of this for the Scottish Chapter members, would feel inappropriate; consequently, I'll briefly add to the mountains of comment.

Almost all predictions and opinion polls show consumer behaviour to be that of reining in expenditure, paying off debt and trying to build savings. As a result, it might be assumed that membership of professional institutions would be one area in which professionals would be looking to cancel expenditure, hence we would be suffering from a reduction in Chapter members. Recent evidence suggests that this is not the case. The Chapter has been growing at a healthy 20% increase in membership per year over the last two years and now has approaching 200 members. Recent months have seen a continuation of this trend to increased new members, as well as renewals running at greater than 90%.

Some thoughts, regarding a few reasons why we may be seeing this ongoing growth, are as follows: in a scenario where people anticipate they may find themselves out of work, the value of memberships in demonstrating professional competence to potential new employers rises. In a scenario where employers are making cuts in staffing numbers, being able to demonstrate competence and continuing development through professional membership may be a marginal factor in deciding where an axe will fall; i.e. it will not stop the numbers from going but may impact on which individuals do go. The value of ongoing Chapter membership and certification to professionals has, arguably, never been so critical.

Considered from a slightly broader context, there has been much discussion that the recession, brought on by the initial financial system meltdown, was a consequence of regulatory failure. In this environment, whether boards want to be seen to axe regulatory functions within their organisations is open to question. Several well-known major Scottish firms have continued to build their audit and governance functions whilst the wider business has faced cuts in staffing numbers. There could certainly be worse areas for us to be working in at present.

Hopefully the above points at least slightly temper some of the overwhelming doom and gloom that seems to dominate coverage at present.

On top of the above points the ongoing work of the Chapter committee, in keeping the programme of educational and training events both relevant and useful, together with the effective communication framework put in place over recent years, can only have helped the Chapter to grow. I would like to personally again thank them for their efforts and also encourage any of the wider membership who would like to get involved to contact us.

Tony Povoas
Director of Consultancy, commissum
president@isaca-scotland.org.uk

Recent Chapter events

Craig Armour and Simon Clifford

Over the past few months, the Chapter has held two evening events for members, both of which were well attended and explored some of the more unusual topics that members might encounter in their work.

Craig Armour of Deloitte presented the October 2008 event at their Glasgow office, looking at how Voice over IP (VoIP) can be secured, whilst balancing against the need to preserve quality of service for VoIP users.

Simon Clifford of commissum presented the December 2008 event, hosted by AEGON UK, exploring issues that arise when planning or using server virtualisation within an existing network infrastructure, and considering the particular security issues that can arise.

Members can access a copy of the presentation slides from both of these events on the Chapter website. These are password protected, so please contact webmaster@isaca-scotland.org.uk if you require a reminder of this.

The Chapter will be holding more events in the near future, so please look out for these.

ISACA updates

Brian Frenkel

Board Nominations

Nominations for positions on the 2009-2010 ISACA Board of Directors have now closed. The Nominating Committee will review all applications and select a proposed slate of board members, which will be communicated to members in the May 2009 issue of Global Communiqué.

2009-2010 Key Boards and Committees

ISACA and the IT Governance Institute (ITGI) rely heavily on their key boards and committees to ensure the continuation of high-quality resources. These groups are made up of volunteers from ISACA's membership. ISACA and ITGI are now accepting applications to participate on key boards and committees for the 2009-10 administrative term. The selection of members for service is based upon the current needs of those groups, the relevant professional background of the candidates and the need to reflect a global perspective. All appointments are for a one-year term. Applications have now closed for these bodies.

Distance Learning Update

ISACA's March e-Symposium was run on Tuesday, 31 March 2009. To register for the e-Symposium program and take the first step toward earning three free continuing professional education (CPE) credits, please visit isaca.brighttalk.com. All e-symposia are recorded and archived for viewing on demand. For more information, please visit www.isaca.org/elearning.

ISACA e-Learning Campus

The CISA Online Review Course is now available on the ISACA e-Learning Campus. This interactive, web-based course provides CISA exam candidates and ISACA members with an efficient, cost-effective tool for exam preparation and for performing information systems audits and reviews. For information, visit www.isaca.org/elearning.

CISA and CISM in the News

The CISM certification has been ranked as the third highest-paying certification in Certification Magazine's 2008 Salary Survey, behind two highly specialised computer networking qualifications.

According to BankInfosecurity.com, industry recruitment experts and information security professionals noted CISA and CISM as two of the top five certifications for 2009, as they provide assurance that the holder has extensive experience in their fields above and beyond passing a test. ISACA's new CGEIT designation is also mentioned as a top certification to earn in 2009.

CISA and CISM Exam Highlights

The results of the December 2008 exams were released by one-time e-mail notification, posted to individual candidate profiles on the ISACA web site and sent by post in early February. To ensure the confidentiality of scores, exam results will not be reported by telephone or fax.

CISA, CISM and CGEIT Applications

To enable ISACA to process applications more efficiently, please collect all application documentation (verification of work experience forms and any applicable university transcript or letter) and send them together in one package to ISACA International Headquarters.

June Exam Registration

ISACA is pleased to offer the CISA exam in Polish beginning with the June 2009 administration. The June 2009 CISA Bulletin of Information (BOI) and 2009 Candidate's Guide are also available in Polish at www.isaca.org/cisaboi and www.isaca.org/cisaguide, respectively.

Registration for the June 2009 CISA, CISM and CGEIT exams continues. The final registration deadline is 8 April 2009. To view additional exam details, please read the CISA, CISM or CGEIT BOI for the June 2009 exams, available at www.isaca.org/cisaboi, www.isaca.org/cismboi and www.isaca.org/cgeitboi.

CISA and CISM Certification Renewals

Certificate holders, who have not already done so, should renew and report CPE hours as soon as possible to avoid revocation. Final reminder invoices have been mailed.

The CPE policies are available at www.isaca.org/cisacpepolicy, www.isaca.org/cismcpepolicy and www.isaca.org/cgeitcpepolicy. The renewal process can be completed online at www.isaca.org and going to "My Renewals."

Getting the perfect job: interviews

Lucy Adam

Regardless of how many interviews you have attended and how comfortable you are with the process, most people (whether they think so or not) can improve with the right preparation. This article looks at how to increase your chances of success in interviews and highlights factors you can influence to your advantage.

When you attend an interview, you are in a competitive arena; rarely will you be the only candidate being considered for the role. This is the particularly the case in the current market conditions, which have resulted in a significant decrease in the number of opportunities available and a greater number of candidates looking for new positions.

To perform well in an interview, it is imperative to create a strong, positive impression while giving a good account of your professional experience, ability and personal attributes. You need to demonstrate your achievements and personal successes, as they are what set you apart from your peers and give you the "X-Factor". Your goal is to assure the interviewer that you can add value to their team and organisation above and beyond the other interviewees, and you have a set period of time in which to do this.

Preparation

Preparing thoroughly beforehand is the best way to instil self-confidence and minimise the likelihood of nerves detracting from your performance.

Basic information

There is no excuse for not ensuring you have the basic information. I would have serious concerns if I interviewed someone not in possession of all of the following:

- The address and directions - if necessary do a trial run out to the location so you are comfortable with how to get there and how much time to allow.
- The name and position of the interviewer.
- A job specification for the role.
- The style, format and duration of the interview.
- A contact number in case you are running late.

Your experience in relation to the role

This preparation presents you with an opportunity to identify relevant experience and attributes that make you a good fit, and to identify skills gaps and think of positive ways to deal with questions in these areas, pre-empting a lack of experience becoming a major issue.

- Review all relevant documents e.g. CV, job specification, team/company structures.
- Identify what you can offer the team/company.
- Identify strengths and weaknesses; turn awareness of weaknesses into a positive e.g. you are taking steps to address a lack of experience in a specific area.
- Think of aspects of your role and the role you are interviewing for that you particularly enjoy.
- If it's a competency-based interview, prepare some examples to use (we will cover these types of interviews in a later newsletter).

The company

There are many sources of company information, including the annual report and accounts, the company website and press centre, online press articles and people you know who work or have worked for the company etc. Be able to answer the following about the company you are interviewing with and your current employer:

- Who owns the company and what is the structure?
- Is the company part of a group - and if so, what are the subsidiaries?
- Who are the competitors?
- What services/products does the firm offer?
- Are they growing, consolidating or contracting?
- How is the company performing financially?

The actual interview

You have arrived on time, you are dressed smartly and appear calm and professional. What else can you do to improve your chances?

First impressions

When you enter the room, hold your head high and go in confidently. Make eye contact and try to smile, however nervous you may feel inside. Shake hands firmly with the interviewer(s) on arrival and again on departure

During the interview, you should sit up straight and try to relax. If you are normally quite expressive and animated, be yourself. If you feel nervous and self-conscious, maintain good eye contact, focus on the interviewer(s) and pay attention to what they are asking you.

Interview technique

Try and suss your interviewer(s) out - there are many types of interviewer and how you respond to them will be influenced by whether or not they are experienced, talkative or monosyllabic, on the ball or unprepared etc. Use those finely-tuned people skills you have developed in your IT Audit career to determine what their interview style is. The following tips apply to all interviews:

- Try to build a rapport but avoid over-familiarity.
- Be positive but not over-enthusiastic.
- Sell yourself but don't be arrogant.
- Convey your interest in the role and organisation.
- Listen to the interviewer and don't interrupt.
- Avoid slang and filler/stalling words such as "like", "basically", "erm" etc.
- Give examples where appropriate to avoid giving general answers.
- If a question is ambiguous, ask the interviewer to clarify.

Standard interview questions

The following is a list of a few questions that tend to crop up often. A much more comprehensive list and advice about how to answer specific questions is available on request:

- Why are you interested in this role?
- What do you know about us/the role?
- Take me through your CV.
- What do you most enjoy/find most frustrating about your current role?
- What have you done that shows initiative?
- How do you cope with routine work?
- What have been your three main achievements?
- What are your strengths?
- What are your weaknesses?
- What skills do you need to develop/work on?
- What motivates you?
- How do you react under pressure?
- How do you deal with criticism?
- What do you do for enjoyment in your leisure time?
- What supervisory experience do you have?
- Describe your management style.
- What are the main skills/traits of a good internal auditor?
- What are the key issues facing internal audit?
- What do you think are the key technology risks our company is currently facing?
- What impact do you think ………… will have on our business?
- How do you keep up with developments in your field?
- Do you prefer to work alone or in a team?
- What skills and personal qualities have you contributed to teams you have been part of?
- How do you see your career progressing?
- What are your short/long-term goals?
- Why do you want to leave your current role? (remember not to be negative about your current employer)
- Why have you changed jobs frequently?
- What other opportunities are you looking at just now?
- Why should we hire you?

If the interview is competency-based, the employer is looking for evidence to support specific competencies they have identified as being important to the role. We will discuss in more detail in a later newsletter.

Your questions

You will usually be given the chance to ask questions. Some good questions include:

- Why do you (the interviewer) enjoy working for this team/company?
- Why did you (the interviewer) join the company?
- Why has this position arisen?
- What is the performance appraisal process?
- What do you think gives this company an edge over its competitors?
- What is the work environment like?
- What are the opportunities for training and professional development like?
- How is the audit function perceived by the business?
- How do you target audits for inclusion in the plan?
- How do you work with business auditors to provide integrated audits?

However, some questions to avoid if you want the job:

- Will I have to work overtime?
- What was the bonus last year?
- When can I expect promotion?
- What holidays are there and can they be traded?
- What is your disciplinary procedure?

Closing the meeting

This is your final chance to leave a good impression! Ask if they have any more questions and what the next step is in the process. Make sure to thank them for their time, shake hands again and remain positive, however you felt you performed in the interview.

Interview clangers to avoid

Lack of preparation

Do your research and memorise key facts and figures, be able to talk through your CV including dates, responsibilities and key achievements.

Answering questions poorly

Make sure you are actually answering what you were asked - listen to the question. Be concise and do not talk for too long, but also do not give monosyllabic answers. Try and build a rapport and avoid appearing too relaxed, as this could be perceived as complacency or arrogance.

Not being prepared for the unexpected

Remain composed at all times - don't let a curve-ball question throw you! Attempt to answer every question and try to turn questions about something negative into a positive e.g. "I have had a problem with ………… in the past but since working to address it, I've not had any issues."

Lying

Do not exaggerate your contribution to a project or your skills and knowledge - it will come back to bite you. Be honest about everything including your experience and skills, reasons for leaving, medical history, how much you are prepared to travel etc.

If you are caught telling a fib, or the interviewer spots inconsistencies, they will have every reason to question your integrity.

Creating a poor first impression

Be punctual, turn off your mobile, give a firm handshake and make eye contact. Above all, don't let nerves affect your performance.

Not maintaining a positive impression

Stay positive at all times - do not badmouth previous employers, disclose inappropriate information or become disheartened if you think the interview could be going better.

Conclusion

Hopefully these pointers will provide a good starting point should you be invited to attend an interview. If you wish to discuss any of the above or if you want more information on competency based interviews before the next newsletter then please do not hesitate to contact me.

Lucy Adam
Managing Director, Adam Appointments
lucy@adamappointments.co.uk

Airline crashes - A case study for IT security?

Paul Guckian

Airline crashes can be seen as random events that occur infrequently, with devastating consequences when they go seriously wrong. In the past 20 years, plane crashes are more likely to be the result of an accumulation of minor difficulties and seemingly trivial malfunctions, rather than one large event. While reading some airline case studies recently, I found myself asking a rather strange question: "Is there a link between airline crashes and IT security incidents?"

Airline crashes, in the form of case studies, have long formed part of the case study methodology developed by Harvard University and are used extensively in the MBA curriculum around the world. There are a number of reasons that airline crashes make good case studies:

- They are formally investigated, therefore all the facts are in the public domain;
- They centre around the interaction between humans and technology, usually under difficult circumstances;
- Their consequences are so severe that they have prompted corrective action across the whole industry.

Everyone can readily relate to the airline industry and the importance of piloting an airplane safely. In the typical airline crash scenario, there are number of observations:

- The weather is usually poor, bad enough that the pilot feels a bit more stressed than usual.
- The plane is usually behind schedule, so the pilots are hurrying.
- In 52% of crashes, the pilot had been awake for more than 12 hours so was likely to be tired.
- In 44% of crashes, pilot and co-pilot have never flown together, so may be uncomfortable with each other.
- The typical accident involves seven consecutive human errors of communication and teamwork.

So what are the lessons for the IT security industry and the auditors who review their work? Can we imagine scenarios where stress levels are increased, projects are behind schedule, where staff are regularly awake for more than twelve hours and people who have never previously worked together are responsible for delivery? In my experience, this is pretty much a typical day in any large company delivering transformational changes.

As one example, in January 2008, Société Générale discovered approximately €7bn ($10.26bn) of losses. It was reported that inadequate IT security allowed Jerome Kerviel, a trader at the Paris-based bank, to make a series of unauthorised transactions that ultimately cost the bank $7.2bn. There are a number of interesting observations:

- Kerviel had previously worked in the bank's IT department and had in-depth knowledge of its systems and procedures. This would not be a normal career progression for traders.
- Staff mostly followed those procedures, but these were not sufficient to identify the fraud earlier. This was partly because of the effort Kerviel made to avoid detection, and partly because staff did not systematically investigate when warnings were raised.
- Kerviel borrowed colleagues' log-in credentials to conduct trades in their names.
- Investigators identified at least seven occasions on which Kerviel had faked messages between April 2007 and January 2008, four of them referring to trades that never existed. The deception was eventually uncovered when they could find no trace of these purported messages in the SocGen archive system.
- Between July 2006 and September 2007, internal controls recorded 24 instances of Kerviel's trades exceeding authorised limits, which were reported by the General Inspection department. At the time, the bank's risk-monitoring unit had put the anomalies down to problems with the way the trading software recorded operations and asked Kerviel's superiors to make sure he didn't exceed limits again.

Here we see a number of relatively trivial events, which occur every day in any investment bank, and yet nobody put them together until the markets moved the wrong way. The billionaire investor, Warren Buffett, once famously said: "It's only when the tide goes out that you learn who's been swimming naked."

Was this the first time that this has happened? No. We can probably recall Nick Leeson's disastrous £600m loss at Barings in 1995, resulting in the failure of the bank. City expert David Buik told Sky News, in the aftermath of Société Générale, that while rules and regulations had been tightened up greatly since the Nick Leeson event, such things could still happen.

In 2007, a phishing attack gave identity thieves access to personal information of 1.3 million Monster.com users. Client machines were compromised by a trojan that gained access to the "Monster for Employers" area of the site. The question is whether Monster are responsible for the breach, or the clients, whose machines were compromised to enable the attacks? Michael Sutton of SPI Dynamics argued that "Both sides certainly played a role, but given the fact that Monster allows anyone willing to set up an employer account to access millions of confidential records, and do so in an automated fashion, it is clear that Monster needs to change its practices to prevent future attacks. Without such changes, we will only need to wait until another Monster client account is compromised before we hear of a future attack." Clearly, nobody thought that one compromised machine could give rise to a huge loss of data. So what are the options to tackle such a complex issue?

In a study of social behaviour, a researcher called Geert Hofstede introduced the Power Distance Index (PDI), concerning attitudes to hierarchy, and specifically how much a culture values and respects authority. South Korea has the second highest PDI rating, with Korean Air having a disproportionate number of airline crashes in the 1990s, compared with the world average. By listening to the recordings just before crashes, it was determined that this cultural behaviour was so ingrained in Korean co-pilots, that they would not overrule their pilot even in the face of certain death.

In 2000, Korean Air finally acted, bringing in an outsider to run their flight operations. David Greenberg, a former Vice President for Delta Airlines, took an unusual first step by evaluating the English language skills of the flight crews, then implementing a language-training program. The second step was to appoint Alteon Training, a subsidiary of Boeing, to manage the training and instruction programme with English as the only communication language. Greenberg established one simple rule: the language of flight was English and every pilot had to be fluent in English. The outcome was to transform the relationship between pilots and co-pilots by giving them a secondary “English” personality, outside the hierarchical Korean culture, which allowed them to communicate better in a crisis. This ultimately reduced the number of crashes.

If we consider the development of Internal Audit in the last few years, we note that the role of the auditor is to provide an independent opinion to the board, by-passing the hierarchical structures of management. This has created secondary opinions, where the hierarchal nature of companies is removed from the equation much like what Greenberg achieved at Korean Air. This meant that issues, previously hidden at a local level, could now reach senior management. This control process is embedded in regulations for all large UK companies.

The study of airline crashes shows that its not just technical skills which ensure success: Korean pilots/co-pilots were just as skilled as American crews, who have the best safety record. In the moment, it was an issue of communication. Prior to the event, it was about identifying and resolving seemingly trivial incidents to minimise the risk of accidents. Maybe by addressing seemingly trivial issues, we can begin to understand the complexity of what causes security incidents.

Nassim Taleb’s 2007 book, “The Black Swan”, studies the impact of highly improbable events called “black swan” events, based on Taleb’s experience as a stock market trader. His book focuses on outliers, events that were outside the normal behaviour or trend. When the regulators recently said that their models didn’t cover the credit crunch scenario, we can begin to see the role of outliers in serious incidents.

It is no accident that the ISO38500 IT Governance standard suggests the principals of responsibility, conformance and human behaviour as three of the key pillars of good technology governance. Can we take lessons from the airline industry and use them in relation to information security and governance? We need to ask:

- How do we manage seemingly trivial security risks upfront;
- How should we empower junior members of staff to speak up;
- How is the company’s hierarchy is structured to improve communication?
- How will communication be managed in a crisis?

One of the challenges, for every company, is knowing when we avoided random events, and establishing whether luck or planning avoided these events.

Paul Guckian
Director, Delaney Consulting Ltd
paul.guckian@delaneyconsulting.co.uk

Acts of imagination

Andrew Richardson

One of the stories to come out in December 2008 involved a group of security researchers and how they managed create a forged digital certificate.

One of the most common uses of digital certificates is for validating a web site prior to making a secure HTTPS-based connection. Without digital certificates, we would not have the extensive worldwide eCommerce infrastructure we have today.

In this scenario, a web browser utilises public key cryptography[1] to validate that a TSL/SSL[2] web server is authentic and that the web site is what it claims to be, so that the user can be happy that they are interacting securely with the web site.

A web site operator obtains a certificate by providing some standard information[3] in an application to a Certificate Authority. Without going into too much detail, this information is then hashed[4] and encrypted with the requester's private key. The Certificate Authority decrypt the certificate request with the requester's public key and hash the information themselves to confirm that the hash values are the same. The Certification Authority makes a number of checks (verifying TCP/IP addresses, telephoning the company etc.) to ensure the requester is who they say they are and, if they are satisfied, they issue a new certificate.

The certificate is then sent back to the requester where, in the case of a web server, it's installed on the server. When a third party wants to establish a secure connection with the web server, the server provides the certificate to the web browser, saying this is who it is, and that the trusted Certification Authority has confirmed their identity. The web browser then looks in its store of certificate authorities for the matching authority that has signed it. The web browser is able to verify that this is a proper signature and duplicates the signing process to verify that they get the same result. It is secure because, if the certificate has been changed in any way, then its hash will have changed.

There are a number of different hash functions which can be used, but the one we are concerned with in this article is called MD5. The MD5 hash was designed by Ron Rivest in 1991 and has had known minor flaws since 1996, but in 2004 some serious flaws were discovered.

As hashes are not perfect, it is possible - but practically unlikely - for two different messages to produce the same hash: this is known as a “collision”. Avoiding some very technical explanations[5], in 2007 some security researchers worked out how they could create a common hash by appending their own carefully designed data to the bottom of two different texts.

So far, so good...

In 2008 a separate group of seven security researchers[6] had a spark of imagination and decided to try and create a “forged” certificate. However, they would need a Certification Authority to send them a digital certificate that they would be able to “lift” the signature from and place on their own “forged” certificate.

Some things were beyond the control of the researcher - digital certificates have a serial number and validity dates. They created a bot and collected about 100,000 certificates which they could then analyse. Analysing these certificates revealed that one Certification Authority was using a sequential number for its serial number. Therefore it would be possible to predict the serial number. Who would have imagined that this could be an issue?

They then created the certificate that they wanted to have forged and the certificate that they wanted to be issue and then worked out what needed to be added to the end of those in order to get the MD5 hash to match. This was important as the certificate authority was going to sign the resulting certificate that would be issued to them, and they would never have the Certification Authority's private key to sign the certificate. But, if their forged certificate had the same hash as one that was signed, then the signature could be used for the forged certificate.

Working out what needed to be added in order to get the hashes to match requires some pretty hefty computation and that's where the Sony PlayStation 3 comes in.

PS3s are designed to handle complex graphics computations and the researchers harnessed the power of an array of 200 PS3s It took the 200 PS3s one-to-two days to complete the required computation.

Once they had created the two certificates they had to get the timing right in order to get the predicted serial number on the issued certificate; this they managed without too much problem, as they got the correct serial number on the fourth attempt. Once they had the issued certificate, the could edit the “forged” certificate and attached the Certification Authority signature. The hashes had been designed to match and so the forged certificate was “valid”.

To add a final flourish, there is a bit in the X.509 specification which specifies if the certificate holder is a Certification Authority or not. The researchers turned this on. Now they didn’t just have one fraudulent certificate: they could now create as many web site certificates they wished.

But what are the implications of all this for IT Auditors and Information Security Professionals? As far we know, this is the only example of someone using this technique to forge digital certificates, but this doesn’t mean it hasn’t already been done. If a large number of PS3s are not available, then a botnets could be used to distribute the computation required for this vulnerability. Has someone else out there had the imagination to attempt this?

Does this mean we should consider any web site that is certified using an MD5 hash as being suspect? This has implications for companies as they will have to be re-certified. Many customers will not be aware of the vulnerability, but there could be a public boycott of sites that have MD5 hashed certificates, which could result in a loss of revenue for the companies concerned. There is currently no need to panic, and many Certification Authorities are now switching to SHA-1 hashing - the problem is that this is already under attack.

So, is it worth going to all that effort to exploit this vulnerability? Well, you would need approximately £58,000 to buy the PS3s, and the researchers spent $657 on certificates - so we could round that up to £60,000. The current DNS vulnerability[7] - and many ISPs have still not patched their DNS servers - could be used to re-direct people from a valid web site to a fraudulent web site. The fraudulent web site would have a valid certificate, thereby fooling users into thinking it was a genuine web site. Banking web sites are an obvious choice and it would certainly be possible for a fraudulent web site to yield many times more than the £60,000 outlay.

Interestingly, the researchers used a highly automated Certification Authority and were able to issue, cancel and reissue certificates many times. Whilst this process was automated, there seems to have been a lack of controls that would notice this kind of unusual behaviour and flag it up for investigation. Did anyone ever imagine that this would be a problem?

And so...

At 1800 GMT on January 27 1967, three US astronauts, Virgil Grissom, Ed White and Roger Chaffee entered the command module of Apollo 1 in preparation for a test. At around 23:30 a fire broke out in the command module and all three astronauts lost their lives. A fellow astronaut, Frank Borman was on the AS-204 Review Board which investigated the Apollo 1 fire. Borman told the review board that the ultimate cause of the fire was “a failure of imagination.”

As IT Auditors and IT Security Professionals, we mustn’t fall foul of this. It’s often said that the best indicator of what will happen in the future is past events. We should take this into account, but also use our imagination and think the unthinkable.

Andrew Richardson
Information Security Manager (Compliance), AEGON UK
andrew.richardson@aegon.co.uk

References

[1] Public key cryptography is also known as asymmetric cryptography, as the key used to encrypt a message differs from the key used to decrypt it.

[2] TSL - Transport Layer Security. SSL - Secure Sockets Layer.

[3] For more information, please see standard for X.509, the ITU-T standard for a public key infrastructure (PKI) for single sign-on and Privilege Management Infrastructure (PMI).

[4] A cryptographic hash function takes a block of data and returns a fixed-size bit string, known as the hash value. Any change to the data should result in a change the hash value. The data to be encoded is often called the "message" and the hash value is also called the message digest (MD), or simply digest. Hash functions should have four main properties: it is easy to compute the hash for any given data; text cannot be constructed that has a given hash; modifying the message changes its hash; and two different messages do not have the same hash. These are the ideal properties.

[5] The MD5 hash works by using multiples of 512 bit blocks, so if the end of the message (if it is not exactly 512 bits long) is padded out to 512 bits. See en.wikipedia.org/wiki/MD5 for more information.

[6] events.ccc.de/congress/2008/Fahrplan/attachments/1251_md5-collisions-1.0.pdf

[7] www.theregister.co.uk/2008/07/24/dns_exploit_goes_wild/

Auditing in the downturn

Charles Meehan

An economic downturn refocuses strategic objectives, from growth to sustainability. It also changes the thrust of management concerns, from visions to budgets. Bread-and-butter processes, core technology and head-count once again become important and the temper of the times changes from rewarding cutting-edge to cutting rewards.

While it would be too glib to say that this offers opportunities for auditors, it does require us to think ahead of the curve and realign our offerings to the new objectives and the new mood.

The rational business strategy is essentially defensive while protecting the capabilities needed for a return to growth in a better future environment.

This article suggests three areas where we can capitalise on our existing capabilities and add value to emergent trends in the business:

- **Cash is king** so businesses need to focus on improving the use of working capital.
- **IT is still critical** and it becomes more (rather than less) important when a business seeks cost savings across the board.
- **Fraud** becomes a more immediate issue than in times of plenty, but staff hiding their mistakes can be a bigger threat to the organisation.

Working capital

The management of working capital is about the control of the “Purchase to Pay” and “Customer to Cash” cycles. Many of these processes have existed in some form since the dawn of trade and have been elaborated alongside the growth of civilisation. So, it comes as a surprise to discover that there remains significant scope for improvement.

Ernst & Young and Danske Bank carried out a working capital management survey in 2008[1] with those responsible for finance and treasury in Denmark's 500 largest companies, updating a similar survey undertaken in 2004[2].

The results of the 2008 survey indicated that 43% of respondents considered that significant scope existed for optimisation of internal processes more or less equally spread across creditor, stock and debtor functions. And 11% thought that compliance with existing processes was one of the areas for improvement. The authors took comfort in the fact that the respondents had identified areas for improvement which would both hit the bottom line and were entirely in their own hands.

Some highlights:

Customer to Cash	
85%	identified scope for improvements in automatic reconciliation of debtor invoicing and payment
29%	did not know what percentage of invoices required manual intervention
57%	believed that invoice handling could improve
33%	invoiced on day of delivery
19%	invoiced over seven days later
40%	did not use credit evaluation tools or confirmed the form of payment when accepting orders
40%	did not use external debt collection agencies

Purchase to Pay	
87%	concluded that their invoice approval process could be improved
67%	believed that the terms of payment could be improved
40%	took cash discounts for prompt payment
30%	restricted purchasing to approved suppliers
55%	used purchase requisitions

Stock	
47%	had a process for removing unmarketable goods from stock
30%	implemented a range of stock management best practices

These results illustrate that there is often scope for improvements to the design and implementation of processes, that could eliminate real money costs. These costs are visible internally as rework and delay, but are often overlooked because of a shortfall in the monitoring and reporting levels of the COSO framework, itself a control shortfall[3]. Surprisingly, companies with the largest volume of customer invoices were not the fastest to issue invoices, nor the fastest to remind customers about payment, suggesting that the quality of information could be the critical factor

One way to achieve some synergy between operational performance and audit delivery may be the embedding of continuous audit tools for use by front line management[4]. The shift is from periodic sampling of the output of the rework and remediation process (i.e. from the "fixed" stuff) to exception alerts produced by monitoring 100% of transactions as input to management control activities[5]. Computer Auditors can add value, both by their contribution to the design of the continuous auditing process and by recommending reductions in other controls as they become redundant.

IT reliability

Business Strategy often positions IT investment as the delivery infrastructure that does the real work for large organisations, through the "household name" ERP offerings with which we are all familiar.

It is a useful reality check to consider the proportion and materiality of the accounting flows which are undertaken "off-line" through what are essentially manual journals and complicated structures of inter-linked spreadsheets. These have not been implemented by the IS department, but by a talented user with Excel VBA skills. These users tend not to have the training to understand the value of a structured approach to development, documentation, quality assurance and oversight. The outputs are posted to the ERP's Nominal Ledger without any audit trail - the default perception is that surely these things are self-documenting.

Identifying and addressing areas, where the reliability of automated processes breaks down, may in some cases involve sophisticated analysis of complex process flows. Manual intervention, however, really simplifies the issue - it nullifies the value of all the system controls up to that point and it may not be possible to devise a system of formal assurance which can rescue the situation.

It is difficult sometimes to know where to begin when dealing with a situation where the users are blissfully unaware that they are the risk. Often, this is first of all an exercise in changing hearts and minds. However, there are sources of help, of which the disaster stories collected by Eusprig may be the most directly useful[6]. In many large organisations, the auditor who can successfully bring some order to this chaos will have done a good year's work for his employer (although it is unlikely that anyone other than their peers will understand the achievement).

This, in turn, raises a generic issue about us. If we do not detect a material error, we struggle to quantify our preventive effect because we feel that the probability of a material loss might be very low. There are three ways of looking at this which may be helpful in formulating our contribution:

a) If the potential loss, the impact, is large enough, it probably does not matter how small that probability is. Unless the business has a voracious risk appetite, a large loss times a very small probability of default is still a material risk.
b) If the loss occurred and you had audited the function but had failed to identify and address the risk, what would be the consequences? (see the AIB/Allfirst case[7])
c) We should make a distinction between risk and uncertainty. Risk, in the sense explained by Frank Knight's 1921 "Risk, Uncertainty and Profit", is an uncertainty that has a predictable likelihood which we can control. If it cannot be reliably predicted and mitigated, then from a business point of view, we need to eliminate the activities giving rise to it - only calculable risk can be priced (see also ISO31000[8]).

In the case of spreadsheet-based systems, there are enterprise solutions which provide users with a fully emulated Excel environment , automatically archiving a version on changes (at selectable levels of granularity), and which enable secure retention and automated change audit in an otherwise manual environment. Such solutions do, of course, have a cost. Unwillingness to meet that cost quantifies risk appetite in this area - they have decided to self-insure for an exposure equivalent to the cost. That is a management judgement: the auditor's role is to ensure that the manager is informed about the relative risk costs so that a decision can be made with knowledge of the facts.

Does your business advertise for non-IS staff with VBA skills? How were daily business critical actions, such as releasing BACS transfers, undertaken on the day when a combination of leave/training/management conference/ sickness meant that no-one on the authorisation list was present? How would you even find out?

Fraud and cover-ups

These risks occur together because they share the need to avoid discovery and are equally difficult to detect. By design, the transactions seek to appear as legitimate, even routine, transactions.

Historically, auditors expect fraud to increase in worsening economic circumstances for two reasons: one is that reduced personal circumstances push some to exploit criminal opportunities that have always been available to them, while the other is that, as volumes of normal activity fall, fraudulent transactions stand out more and are easier to spot (the "Bernard Madoff scenario").

Most serious fraud in large organisations requires a minimum level of authority and will often involve a small group of people. Because they look like ordinary transactions, they are seldom detected by Internal Auditors, but they will exploit weaknesses in controls which are well known to insiders. The control weaknesses can often be traced to poor quality master data - unverifiable addresses, incomplete records and duplicated identities. The extent of the information quality shortfall can, however, be quantified in order to sensitise everyone to the risk and there are some types of checking which can usefully be added to computer audit programmes as a matter of routine[9].

Surprisingly, it is the big cover-up rather than a fraud which can destroy a business; Barings Bank, Enron and Société Générale are just a selection of the coverups that became large frauds driven by fear of exposure rather than the desire to steal. This provides the fraud with a measure of protection from discovery until the scale becomes too large to avoid. The perpetrators do not see themselves as acting dishonestly within their business context, but rather trying to protect their reputation[10]. However all of these cases involved fraudulently altering reconciliations and all of them were possible only by ignoring basic good practice, such as segregation of duties or, particularly in Finance, requiring staff to take a block of leave at least annually.

How often do we identify people who do not take up their leave entitlement and those who never take a week or more off at a time? Indeed, how often do we map errors and inconsistencies identified in ERP transactions to specific users rather than to sections? How might we know when supervisor level access is being used by subordinates to get critical activities done in their manager's absence? Similarly, discovering that an ERP user has left, how easy is it to check when their system access was revoked? Beyond that, how easy is it to look in the system logs for use of their system access after the date of their departure?

We may need to source information from the HR and access control elements of systems in order to do a finance audit which stands a chance of detecting fraud or a big cover-up, but having used audits to identify the issues, the preferred solution should be to have these checks embedded in applications so that they generate management alerts in real time.

Charlie Meehan
Treasurer, ISACA Scottish Chapter
treasurer@isaca-scotland.org.uk

References

[1] Storgard, P. Larsen, SL. 2008. Where is the greatest potential for improving working capital? www.gtnews.com/article/7497.cfm (free registration required)

[2] gtnews.com. REL Consultancy. Citigroup. 2004. Operational cash 2004: Insights into working capital. www.bit.ly/isc-cm01

[3] COSO. 2004. Enterprise risk management - integrated framework. www.bit.ly/isc-cm03

[4] GTAG 3: Continuous auditing: Implications for assurance, monitoring, and risk assessment. wwwbit.ly/isc-cm02

[5] University of Minnesota. 2007. Data mining and continuous auditing. www.bit.ly/isc-cm04

[6] Spreadsheet mistakes - news stories. www.eusprig.org/stories.htm

[7] Butler, R. 2002. The role of spreadsheets in the AIB/Allfirst Fraud. www.bit.ly/isc-cm06

[8] ISO TMB WG. 2007. Committee Draft of ISO31000. www.bit.ly/isc-cm05

[9] Kusnierz, R. 2006. Data mining for fraud. www.asis.org.uk/documents/ Data_Mining.pdf

[10] Connor, D. 2008. How to lose $7.2bn with just a few basic skills. www.bit.ly/isc-cm07

Chapter and Local Events

30 April 2009

IIA Scottish District event: Financial Audit Forum - Financial Controls

KPMG, Castle Terrace, Edinburgh
Speakers TBA

Information on IIA Scottish District events - e-mail jpthomson@tiscali.co.uk

15 May 2009

BCS Glasgow Branch event: Mobile Computing

The Lord Todd, University of Strathclyde, Glasgow
Pete Barrie, Director, Mobile & Ubiquitous Computing Research Group, Glasgow Caledonian University

Information on BCS Glasgow Branch events - available at www.glasgow.bcs.org.uk

9 June 2009

ISACA Scottish Chapter: AGM

ISACA Scottish Chapter training event: Working with Third Parties (7 CPEs)

Royal Society of Edinburgh, George Street, Edinburgh
Stan Dormer, Mindgrove

13 June 2009

CISA, CISM and CGEIT exams, to be held in Edinburgh

e-Symposium - available at isaca.brighttalk.com

31 March 2009

Security Vulnerabilities and Safeguards (3 CPEs)

Jeffrey Ritter, CEO, Waters Edge Consulting (Moderator)
John Moynihan, President, Minuteman Governance
Josh Shaul, Director Technology Strategy, Application Security, Inc
Ryan White, Product Marketing Manager SSL, VeriSign
Tim Matthews, Vice President Marketing, PGP Corporation

Archived e-Symposia - available at isaca.brighttalk.com/recorded-events

ISACA Events - more details at www.isaca.org/conferences

15-19 June 2009

ISACA International Training Week (up to 38 CPEs)

Hilton Vienna Plaza, Vienna, Austria

19-22 July 2009

ISACA International Conference (up to 40 CPEs)

Hyatt Regency Century Plaza, Los Angeles, California, USA

To contact the ISACA Scottish Chapter

Tony Povoas (President) - president@isaca-scotland.org.uk
Paul Guckian (Vice President) - vpresident@isaca-scotland.org.uk
Olagbuyi Oduniyi (Secretary) - secretary@isaca-scotland.org.uk
Charles Meehan (Treasurer) - treasurer@isaca-scotland.org.uk
Alan Rennie (Membership) - membership@isaca-scotland.org.uk

For more information about this newsletter, or to contribute articles

Guy Lomas (Newsletter Editor) - newsletter@isaca-scotland.org.uk