The top articles for Risk Professionals seeking up-to-date knowledge of key regulation and compliance.

Volume 1

CYBER CRIME AND IT RISK

The world's premier online risk forum for professionals and services providers

Compiled by:
Boris Agranovich
Founder of Global Risk Community
Copyrights

All rights reserved by the authors

To view our privacy policy, click the link below:

Privacy Policy
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copyrights</td>
<td>2</td>
</tr>
<tr>
<td>Contents</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Is Cybersecurity an Inside Job?</td>
<td>8</td>
</tr>
<tr>
<td>The Enemy Within</td>
<td>8</td>
</tr>
<tr>
<td>What We Don’t See Can Hurt Us</td>
<td>10</td>
</tr>
<tr>
<td>Cost Justifying Security Through Anomaly Detection Process Efficiencies</td>
<td>12</td>
</tr>
<tr>
<td>Conclusion</td>
<td>13</td>
</tr>
<tr>
<td>Can a computer virus make you ill?</td>
<td>15</td>
</tr>
<tr>
<td>Security Risks of Web 2.0</td>
<td>17</td>
</tr>
<tr>
<td>Introduction</td>
<td>17</td>
</tr>
<tr>
<td>Some Stats</td>
<td>18</td>
</tr>
<tr>
<td>So what’s the risk?</td>
<td>18</td>
</tr>
<tr>
<td>Phishing Scams</td>
<td>19</td>
</tr>
<tr>
<td>Web-based Malware, exploits and other attacks</td>
<td>19</td>
</tr>
<tr>
<td>Data Breaches and Data Leak</td>
<td>20</td>
</tr>
<tr>
<td>Short Links</td>
<td>20</td>
</tr>
<tr>
<td>What’s the solution?</td>
<td>21</td>
</tr>
<tr>
<td>Risk Management</td>
<td>21</td>
</tr>
<tr>
<td>Policies</td>
<td>22</td>
</tr>
<tr>
<td>Policies need to cover:</td>
<td>22</td>
</tr>
<tr>
<td>User Awareness</td>
<td>22</td>
</tr>
<tr>
<td>Good Endpoint Protection solution</td>
<td>22</td>
</tr>
<tr>
<td>Secured Web Gateway</td>
<td>23</td>
</tr>
</tbody>
</table>
Security issues of cloud computing ................................................................. 24
  1. Cross-reliance trends .............................................................................. 24
  2. New host architecture models ................................................................. 25
  3. Accelerated threats and sophistication of threat advancement .......... 25
  4. Difficulties for law enforcement in keeping up with evolving threat levels 25

What Your Board Should Know About IT Risk Management .......... 27

Why improvement in technology equals greater risk to everyone .... 29

CYSPEX Cyber Security Breakfast: From Threat to Solution - A Success! .......................................................... 32

Compliance new round up ........................................................................ 37
  FSA warns FCA may change discretionary firms .................................. 37
  Pension funds must reduce their estimates .............................................. 37
  EU lawmakers set July 9 vote on market abuse, MiFID directives .... 38
  On-line fraud still a problem for financial services.............................. 39

Striking the balance in data governance ................................................. 41

ERM: 5 Steps to Success ............................................................................ 44
  1. Begin with a "quick win" ....................................................................... 45
  2. Streamline current daily activities ......................................................... 45
  3. Make relationships visible .................................................................... 46
  4. Use risk assessment tools to prioritize tasks ....................................... 47
  5. Establish the ERM Process .................................................................. 48

So what is holding you back from getting started? .............................. 48

Good vs Bad control .................................................................................. 50

Mobile Betting News: Mobile Crime & Fraud Risks ....................... 51
  Eugene Kaspersky, Founder of Kaspersky ............................................. 51
  Features ................................................................................................... 51
  Metrics ..................................................................................................... 52

Japanese Nuclear Crisis: lessons for risk managers ....................... 53
CONTENTS

Link controls to the assets they depend on.......................................................... 53
Evaluate risk impact for each business process................................................. 54
Routinely revisit risk assumptions to reveal emerging risks............................. 55
Evaluate risk from vendor relationships............................................................. 55
Big Data...Big Deal? ............................................................................................. 57
Introduction

The third book in the Global Risk Series is dedicated to IT and Cyber Risks.

Rapidly changing and advanced technologies are making it increasingly difficult for companies and governments to manage and secure confidential data.

According to the 2014 Global Risk report compiled by the World Economic forum, the technological risks of cyber attacks, data fraud/theft and critical information infrastructure breakdown are strongly connected to each other and to risks such as terrorist attacks and global governance failure.

Fresh thinking at all levels on how to preserve, protect and govern the common good of a trusted cyberspace must be developed.

Learn from some top experts in the industry as they explain major IT and Cyber security issues and ways how to address them. Check out their tips and use the links at the end of each article to navigate back to the website to leave your comment or ask a question.

Special thanks go to members who contributed to this report: Larry Karisny, Michael C. Thomsett,
Biji Scaria, Steven Minsky, Rebecca Beard, Edwin Etadafe, Norbert Boon, Lesego, Jacques LeDisco, Sebastien Jaouen.
While security clearance and authentication processes are essential to physical and other security, the physical DC Navy Yard breach by Aaron Alexis and the state secret breaches by Edward Snowden illustrate some disturbing weaknesses in personal validation and authentication. These clearance breaches were very different in nature but show a range of how a person’s calculated action can subvert basic security measures.

Neither top secret clearance, sophisticated authentication nor the most advanced encrypted information systems can necessarily stop an intended breach action. These security procedures are not designed to detect real-time actions and anomalous business processes from authorized personnel. These practices are just the "moat around the castle" approach upon which most current cybersecurity technologies are based. Current national security breaches clearly show we need to do more.

**The Enemy Within**
The highest percent of breaches occur inside an organization. When a criminal wants something specific
he or she will choose the path of least resistance to obtain it. Cybercriminals don’t do this by breaking complex security algorithms. They normally do it by gaining access as a trusted insider, using and manipulating secured and authorized software and hardware to which they have access.

Corporate espionage has utilized this methodology for years and now entire countries are using software exploits to gain access to state secrets in this new cyberwar. Authenticated access is not the issue. The unknown enemy already has access. We need to quit focusing so much on allowing and disallowing access and instead watch the business system process tools and how people are using them.

As our organizational systems grow larger and our business process and control systems become more complex and connected, we begin to lose track of what we are doing, let alone securing what we are doing. We currently run business processes using layers of software, hardware and people all trying to achieve a certain departmental or subsystem task. Whether software, machine or human -- the actions of these process components are seldom if ever combined in a single understandable view of the entire process. By not allowing a total system action view, the breach of a
single process action could greatly affect other connected process actions and potentially take down the whole system.

These process actions are the Achilles heel of cybersecurity and they cannot be defended by hardening physical, network or system information process security. We need to direct our attention more toward action viewing technologies vs. encrypted authorized actions. We need to assume the enemy is already in and needs to be watched.

**What We Don’t See Can Hurt Us**

While many people are very concerned about technical snooping capabilities, the fact is that we need better snooping capabilities in areas such as critical infrastructure, industrial control systems, intellectual property and national defense. We have created massive intelligence process capabilities through computer software, hardware and networks and have done a pretty good job securing the transport and storage of information but little in securing system processes. When we interconnect multiple actions to multiple processes without detection capabilities, we leave a wide open opportunity for breaches. Physical security in background checks, biometric authentication, RFID location based services and network encryption all have
value, but they alone will not stop an authenticated breach. We are not even looking in the right place.

The recent national security breaches were recognized at the action output level after the breach action already occurred. These breaches demonstrate two very important requirements in security that we must be concerned with. One is that we need to add intelligence to physical, human and machine actions that view and even predict a physical breach like a person breaking barricades. We can’t just go back to the old days and think that getting rid of all this digital smart stuff will improve security. It won’t. These intelligent and connected technologies can greatly help both physical and digital security if properly implemented. There are a multitude of technologies that can give intelligence to our physical world.

The second important requirement is the timing of when a process action breach occurs versus when a process breach can be observed and blocked. This is where new technologies such as anomaly detection can be used to recognize, audit and block these process actions at the real-time data input level when seconds matter. The technologies exist and are called anomaly detection. Companies such as IBM and Decision Zone have so much belief in these technologies that they have both patented
their solutions. When things aren’t working properly, demonstrated by the scale and magnitude of the cyber breaches we see today, we need to do something different and there are some security companies that are realizing this. So the big question is how much? The answer may surprise you.

Cost Justifying Security Through Anomaly Detection Process Efficiencies

One of the biggest concerns in security services is the initial cost in deploying these technologies, the continued cost in using them and how these costs can be justified. Even improvements in first-level authentication and IT security are not yet considered a cost of doing business although these opinions are changing. There are ROI calculators that are now at least trying to put a number on the cost of potential security breaches and attempts to reduce insurance policy premiums when cybersecurity defensive plans can be demonstrated.

Security is only the anomaly detection of an incorrect process action. More accurately viewing the process actions through anomaly detection can also improve the total process. Security is really only a byproduct of detecting anomaly actions that are not part of the process. People are not buying security because they can’t justify the cost. Both the public and private sectors
can gain efficiencies through the use of anomaly detection resulting in service savings or profit that would justify the cost of security. The process efficiencies gained through anomaly detection technologies can absorb the cost of security while improving process actions.

**Conclusion**

Problems occur in business processes when someone or some technology does something wrong whether intentional, mistakenly or as part of a targeted attack. We can only achieve true security when multiple actions and process can be detected simultaneously and in real time. New technologies are offering these capabilities in a time when we are rapidly expanding interconnected humans to intelligent machines that have capabilities that are so large we are having trouble even viewing these processes.

We need to start recognizing that authentication of a person no matter how accurate the techniques used are only the first level of cybersecurity. True security can only be achieved when combining prevention and detection technologies at the real time business or process input action level. Most security breaches occur quickly and are themselves an input process action.
Using technology than can focus on these input actions is where we need to focus our efforts.

True cybersecurity will be obtained when we can effectively view, audit, correct and block organizational process actions. If you could have a technology that does this, then why not?

Read this article on the website [Click Here](#)
Can a computer virus make you ill?

How can we plan for a risk that is not even known? The answer, of course, is that we cannot. Planning by nature has to be aimed at managing losses resulting from unknown and unthinkable disasters.

For example, an organization needing to protect its proprietary assets may be wise to diversify its storage and even access to counter potential losses from cyber attack, industrial espionage or internal sabotage.

What happens when the entire system is down for an extended period of time? In the early days of computerization, companies used to employ a back-up consisting of old-style hand entry and storage of data. I can even recall working for a company in which my manager gave me a massive monthly print-out from the “computer department” and had me check the math. The trust level in those days was low, and managers did not understand what computerization was all about. Today back-up has to be more comprehensive and sophisticated, but we still need it.

Are we better off today? Maybe not. Everyone knows how online and IT stuff works, but from the perspective of
risk management we are more vulnerable now, not less. We are so dependent on automation for so much, that a system-wide failure makes us helpless and robs us of even the most basic information.

I have focused in past blogs on the potential threat of pandemic as both a health and supply chain issue. But perhaps the next pandemic threat will come from an online infection and not from an actual viral or bacterial attack. A few years ago, I saw a letter written to a local newspaper from someone who had heard about a computer virus. The writer asked, “Can this make me and my family sick?”

It might sound funny, but as it turns out, it could be the most important question risk managers can ask, especially when it comes to protecting IT assets.

Read this article on the website Click Here
Introduction

Let’s start with what’s Web 2.0 before getting into the risks.

The term Web 2.0 is commonly associated with web applications that facilitate interactive information sharing, interoperability, user-centered design and collaboration on the World Wide Web.

For some of you still not clear of what’s Web 2.0 let me put it down in a different way. Web 2.0 is Facebook or MySpace or Linkedin or Twitter or the blogs or the Wikis or any web site which allows the visitor to interact by posting updates, comments or uploading pictures or videos.

The biggest challenge of the Web 2.0 world is that security must focus on protecting open systems rather than shutting everyone out. The social networking tools built on web and web 2.0 are incredibly powerful and useful: in some cases it can make employees more productive and speed up decision-making and in some cases they can allow companies to gain a competitive
advantage over their rivals, and they can significantly reduce the cost of doing business.

**Some Stats**
According to a study by global communications firm Burson-Marsteller, more than three-quarters of the Fortune Global 100 companies are using at least one of the most popular social media platforms (Twitter, Facebook, YouTube, and corporate blogs) to actively engage with stakeholders. Sixty-five percent of the largest 100 international companies have active accounts on Twitter, 54 percent have a Facebook fan page, 50 percent have a YouTube channel, and one-third have corporate blogs.

The Nielsen Wire reports that the world now spends over 100 billion minutes or 22 percent of all time online on social networks and blog sites.

**So what’s the risk?**
The trusted nature of Facebook, MySpace and other social networks allow hackers to launch exploits and spread Web-based malware. Research says that, high number of users click on any link send by their friends in Facebook or MySpace or Linkedin due to the façade of trust these sites have. They won’t exhibit same amount
of caution on social networks as they would when communicating in person.

**Phishing Scams**
I hope most of you are aware of the phishing scams common in email networks and it reached a stage where these techniques are extended to social networks. In email networks users are typically lured to a fake financial institution web site controlled by cybercriminals and once the data is entered into the fake site, it is stolen and used in identity theft crimes.

The open and trusted nature of social networks is making it easier to have same kind of scams and as per security company Kaspersky there were several phishing scams targeting Facebook or MySpace where a user received an email (from a trusted friend) with a link to a groundbreaking news event or an exciting photograph or video. A user clicking on that link is taken to a bogus site that imitates the login page of Facebook or MySpace. The end result is another stolen credential.

**Web-based Malware, exploits and other attacks**
As email is getting more and more secured by having multiple levels of malware protection and spam filtering, majority of malware is today distributed through
websites. The methods could be asking the user to visit a website to get some freebies or to view some amazing video by downloading some plug-in and their by infecting the system. In some cases the malwares will be exploiting the known or zero day vulnerabilities identified in the operating system or other software’s (Flash, Adobe, Java etc) users use.

The malwares entering the system this way will have the capability to steal sensitive information from a computer or make the system part of a botnet network.

Data Breaches and Data Leak
Inadvertent data breaches can occur when users use Web 2.0 tools. This could be the case where a user accidently entering some sensitive information on the web that can harm the reputation of his or her employer or inform the world of some confidential activity.

It’s possible to leak Sensitive or confidential information through social network or through social network based instant messaging

Short Links
Due to the extensive use of status update sites, blogging sites and microblogging sites like Twitter, use of URL/Link shortening is very popular and this creates a security risk where end user has no way of knowing
what is on the other end of the shortened link without clicking on it. This gives cybercriminals the potential to send legitimate sounding links that actually lead to malicious sites.

**What’s the solution?**

**Risk Management**
The first step in risk management is to understand the type of risks organizations facing from the variety of Web, Web 2.0 and social networking threats and the nature of these threats. This can vary from organization to organization and user group to user group. Use publically available sources to provide this education, including vendors of Web security gateways, industry analysts, consultants, speakers at trade shows, Webinars etc. The key for any Security Manager is to educate himself or herself about the nature of the threats, how they could specifically impact their organization, and the remedies that are available to prevent and/or remediate them.

The next step is to carry out a detailed audit of the organization’s Web and endpoint security controls. The goal is to identify the holes in the security systems and to see what protection method is implemented. The result of this audit should be a vulnerability assessment
that clearly defines where the system/user/network is protected and where it is vulnerable to attack and the criticality of the risk.

**Policies**
Depends on your organizations requirements, make sure you have clearly defined policies on what’s allowed and what’s not allowed. Based on the policies, educate employees on safety and security, and provide a framework for managing violations.

**Policies need to cover:**
Details of monitoring and blocking in place, content users are allowed to share and services part of social networking allowed.

**User Awareness**
Educate users about the risks of Web 2.0 and make sure they are aware of all the risks associated. Tell them in the world of Web 2.0 or Social Networking ‘Don’t trust anything’, ‘Challenge everything’ and finally ‘Have your own privacy’. Further make sure users are aware of the existing policies and enforcement process.

**Good Endpoint Protection solution**
Invest in a good endpoint protection solution. The days of having Antivirus and Antispyware protection based on
signature analysis only is gone. Other than the Antivirus and Antispyware protection you need to have an endpoint protection solution which has more features like application & device control, HIDS/HIPS, firewall etc and malware detection capabilities based on signature, heuristics or behavior based.

**Secured Web Gateway**
For web traffic you need to employ malware, content and URL filtering technologies. Organizations need to ensure that all web traffic coming and going is passed through a Secured Web Gateway solution and typically, these security solutions are capable of efficiently thwarting the majority of malware and malicious content that propagates through web 2.0 technologies. Additionally, Data Loss Prevention is an effective tool for monitoring any outbound communications, especially social networking. Using data loss prevention solutions that prevent sensitive data traveling outside the corporate network can be extremely valuable in keeping corporate data from leaking out to a social network either accidentally or intentionally.

Read this article on the website [Click Here](#)
Security issues of cloud computing

Posted by Michael C. Thomsett on September 1, 2011 at 8:27pm

We may all expect that security is going to be as important in the near future as data efficiency. The exciting developments in cloud computing make this two-part challenge glaringly important. Of course everyone wants data efficiency and unlimited, easily accessible storage. However, the future success stories of cloud computing may be those providers able to offer these benefits along with exceptionally high levels of security.

Four areas are likely to dominate the discussion of security in cloud computing:

   One likely outcome to cloud computing will be the increased reliance among private sector companies and public agencies on the cloud, but even more important upon one another as well. As the IT environment expands rapidly, it will cause increased shared interests in the two big sectors, in terms of all aspects to the cloud: data management, processes, storage, retrieval, security, and communications.
2. New host architecture models.
The cloud, like its grandfather the Internet, will clearly be a dynamic set of technological capabilities. The need for improved and higher-level security by itself will cause changes in cloud architecture. However, marketing priorities will also come into play in the ever-evolving nature of the cloud. The new methods are likely to include wireless data transfer, a growing role for social media, and of course the rapid expansion and reliance on hand-held devices as part of the cloud.

3. Accelerated threats and sophistication of threat advancement.
Just as technology advances in a positive manner, so will the threat universe. A black market is already evolving for intellectual property theft and misuse, and in the cloud this is sure to continue. The IT challenge of the future will be to remain steps ahead of threats as the cloud evolves and expands. Man-in-the-middle attacks and domain squatting are likely to be serious issues, but they might also be the tip of the iceberg.

4. Difficulties for law enforcement in keeping up with evolving threat levels.
By definition law enforcement is most often responsive. Given the rapid growth of cloud technology and its global
attributes, this problem is going to become more severe in the future. Unfortunately, cyber crime is becoming very profitable, and law enforcement will need to step up its cooperative efforts with industry and government to figure out how to curtail these activities.

Read this article on the website Click Here
Recently organizations have been faced with the increasing threat of cyber attacks, whether from external hackers such as lulzsec or from internal attacks such as wikileaks. Your customers' personally identifiable information, organization's intellectual property, and confidential files are all vulnerable to attack.

How prepared is your IT Risk Management? How vulnerable is your organization to a cyber-attack? What would the consequences of a cyber-attack be on your organization? Your board needs to know.

The consequences of a successful cyber-attack reach far beyond just legal or IT issues. An organization's reputation, customer loyalty, and ultimately strategic goals will suffer as a result deeply affecting the bottom-line.

A prime example is recent the Play Station Network breach earlier this year. The security breach forced Sony to shut down their network for over a month disrupting Sony’s revenue, operations, and possibly even future
sales. What will ultimately hurt Sony as a result of the breach won’t be the legal ramifications or the cost of implementing better IT security. It will be the breach’s long-term effects on customer loyalty, reputation, and even market share.

What would be the consequences of a data breach or other cyber-attack be on your organization? Are you prepared for an attack beyond IT resiliency?

With such high-publicity breaches at Sony, Epsilon, Lockheed Martin, and even the U.S. Chamber of Commerce, your board will want to know if your organization faces the same risks. What Should You Present to the Board?

If you're unsure of what information you should report to the board, you can watch our complimentary on-demand webinar Presenting Risk Management to the Board.

Read this article on the website Click Here
The miracles of modern technology have made everything faster, easier, more global. But these have also made everyone in the global supply chain critically vulnerable -- not just to the risks we all knew about two decades ago, but to many more, new risks that may cripple us more than ever.

It may not be enough to develop disaster recovery plans, diversify, practice lean and efficient methods, or even to evaluate internal risk management processes constantly. The problem not addressed in all of this is the changed nature of risk itself. In the past, a business model was based on static processes and systems. Today it is all replaced by dynamic models, and this means that simply keeping up with evolving risk is more difficult than ever before. The known risks are constantly evolving and growing, and at the same time, we cannot know about all of the risks out there.

An example: Wal-Mart has over 7 billion customers every day, not to mention 2 million employees and another 3 million additional indirect workers and providers. What happens to all of this if a pandemic strikes? Over 80% of
Wal-Marts goods come from suppliers in Asia and the singular reliance on that supply chain makes the company, its customers and employees all very dependent.

It doesn't have to be a pandemic, either. A severe earthquake, flooding, or cyber attack could just as easily cripple a massive portion of one of the largest supply chains.

The solutions are not easily identified; however, a big part of the problem is denial. Do we assume that someone else has a handle on these new risks and knows how to counter them? Do our subsidiaries, suppliers and manufacturers care about risk to the same degree that we do? Is someone else in charge and is is their problem, not ours?

Disasters are always aggravated when risk managers and others are taken by surprise. Many of today's risks, including the vulnerability of the global supply chain, are linked unavoidably to improved technology. Apart from the known threats like pandemic, earthquake, terrorism, or labor strikes, what about the broader, more profound threat? What happens if the whole cyber-based system we all rely upon is unavailable for more than only a few hours? Who routes the goods, pays for them and gets them onto the shelves? Or, perhaps we should all be
asking, How do we turn the lights back on if and when the most unthinkable disaster occurs?

Thomsett is an author and speaker specializing in business and investing topics. His paper, "Global Supply Chain Risk Management: Viewing the Past to Manage Today's Risks from an Historical Perspective" was presented in December, 2010 at the IntellectBase International Consortium. The paper was then selected for publication in the journal "Review of Management Innovation and Creativity" (February 2011 issue, Vol. 4, Issue 9)

Read this article on the website Click Here
CYSPEX Cyber Security Breakfast: From Threat to Solution - A Success!

Posted by Rebecca Beard on March 5, 2012 at 12:22pm

Is your organisation leveraging the competitive advantage of a positive cyber security culture? What is your organisation doing to promote cyber security and support the Government in making the UK the world's leading market place? It's a fine line between protection and enablement – how is your organisation dealing with the cultural and behavioural impacts?

These questions and more were raised at the CYSPEX Cyber Security Breakfast held at the Houses of Parliament on the 1st March 2012. It was a full house with attendees from the government, private sector and academia providing insights and responses to some of the challenges facing the UK in Cyber Security.
The event was sponsored by Templar Executives and Stratex Systems. Andrew Fitzmaurice, CEO, Templar Executives, introduced the speakers and set the scene explaining, “Today’s briefing is designed to promote the holistic approach required for effective cyber security and to hear from those in the public and private sectors who understand this and are actively contributing to the National Cyber Security Strategy”.

Key note speakers included; Andrew Miller MP and Chair of the Science and Technology Select Committee, Adrian Leppard, Commissioner of Police for the City of London, John Cook, Head of Defence Security and Assurance Services, Ministry of Defence, Simon Parker, Chief Information Officer, Babcock International Group PLC and Rena Lalgie, Deputy Director of Cyber Security, Department for Business Innovation and Skills. Both Baroness Paul Neville-Jones (Special Representative to Business on Cyber Security) and Lord Errol supported the event and participated in the lively audience debate that followed. All of these attendees are prominent in the actions they are taking to develop the UK’s Cyber Security maturity response.

Andrew Miller MP opened the session by highlighting it is imperative for government and business to work together to tackle the cyber threat which is growing and
“increasingly complex and dynamic”. Commissioner Leppard re-enforced this by stating that last year alone, fraud cost the UK economy £38.6billion.

Commissioner Leppard outlined the plans of the Economic Crime Unit and National Fraud Intelligence Agency and the steps they are taking to centralise the capture of fraud intelligence. The Commissioner concluded by saying; “the threat of internet crime is increasing exponentially and whilst both the government and the private sector have responded positively to this challenge we have got to keep the pace going” a view that was echoed by all speakers.

John Cook from the MoD and Simon Parker, CIO of Babcock shared the approach that their respective organisations are taking to increase their Cyber Maturity capability. Simon Parker explained that technology was only part of the picture; to be effective the culture of the organisation needed to be changed by carrying out training, at all levels, to raise awareness. Both the speakers concurred that organisations need to do more to articulate their information risk appetite and manage risk in accordance with that appetite.

John and Simon also emphasised the need for the board to endorse a Cyber Security strategy and drive change from the top. Implementing effective cyber security
requires everyone within an organisation to be accountable and take responsibility for understanding the threats and vulnerabilities they face and how they can prevent them. Addressing the supplier market, John Cook said suppliers need to “take action to ensure and demonstrate they have sufficient cyber security measures in place in what is a dynamic challenge that none of us can afford to ignore.” It was noted that those suppliers who did take action were not only contributing to the overall aim of the National Cyber Security Strategy – making UK Plc the place to do business – but also gaining a competitive advantage.

Rena Lalgie called for a shift in emphasis so that cyber security is seen as an enabler for economic prosperity and that there needs to be a focus on galvanising and partnering with the private sector to deliver the change necessary in this area. Cyber security should be an integral part of how companies manage their corporate risk.

In his closing remarks Andrew Miller MP commented on the next generation of the UK workforce and observed “the missing link is in education; technical and practical skills and behavioural change need to be taught and embedded in the education process. We need to shift the dynamics so young people grow up knowing how to
protect their own work and are used to working in that way."

To find out more about the speakers and CYSPEX please visit the CYSPEX website [www.cypex.com](http://www.cypex.com)
FSA warns FCA may change discretionary firms

The FSA has in recent months warned the Financial Conduct Authority (FCA), which will take over conduct regulation when the FSA is split by the end of the year, will take a more aggressive approach to intervening in the design of financial products. Linda Woodall, head of the savings and investments department at the FSA, told Investment Adviser that “some development” may be required from discretionary fund managers (DFMs) in particular under the FCA regime. “We are not mandating the size and shape of the marketplace,” she added. “The key thing we want to see is good consumer outcomes.” The FSA’s focus on DFMs, and other solutions that financial advisers are using to outsource their investment duties ahead of the RDR, was made clear when it published a guidance consultation on outsourcing last week.

Pension funds must reduce their estimates.

According to the FSA, firms must lower average estimates of a 7% rate of return for investment products that are a mix of equities and bonds to between 5.5% and
6.5%. The recommendation is based on the results of a study by PricewaterhouseCoopers LLP. The projected returns are “reasonable central estimates over a 10-15 year time period,” the report said. The report continued: "The near future remains highly uncertain and we should continue to expect volatility as markets react to any signs of recovery or further weakness. Effective policy actions in the Eurozone are crucial, but analysis of economic trends cannot easily predict the outcome of those decisions. The movements of the key macroeconomic variables over the next five years or so will reflect a process of adjustment back to trend and so are likely to differ from long-term trends."

**EU lawmakers set July 9 vote on market abuse, MiFID directives**

Members of the European Parliament's economy committee will vote July 9 on the European Commission's proposed revisions to the Market Abuse Directive and the Market in Financial Instruments Directive, the EP's press service said Thursday. The revisions to both directives aim to improve transparency and address loopholes in the regulation of derivatives markets, including commodity derivatives and the lack of criminal sanctions for abuse. The market abuse regulation would address gaps in the regulation of over-the-counter trading.
"It was decided that MAD and MiFID legislation should be voted [on] together since they are strongly interlinked," the EP press service said Thursday after the economy committee had its first debate on the Market Abuse Directive.

**On-line fraud still a problem for financial services**
The financial sector continues to be a magnet for frauds and cyber-crime is becoming a major threat as increased internet usage gives rise to scams and data theft, a global survey has found.

Information technology experts say online banking creates fertile ground for frauds who use scams such as phishing to steal clients’ money after obtaining their account details.

Professional services company PricewaterhouseCoopers (PwC) says in its latest global survey on crime: "Most individuals and organisations rely upon the internet and connected technologies, opening themselves up to the risk of attack from global criminals from anywhere in the world."

PwC partner Louis Strydom said up to 40% of respondents in SA had not received cyber crime training or awareness communications of any kind during the past 12 months.
About 46% saw cyber crime as an external threat, he said, warning that companies should recognise the potential internal risk of the crime and prepare themselves accordingly.

"We are experiencing comparable levels of cyber crime to our international counterparts. South African banks are at the forefront of technology and combating cyber crime, but continued vigilance is required," Mr Strydom said yesterday.

Criminals were posing as cellphone company representatives and tricking customers into switching off their phones while they tried to gain access to their bank accounts, the South African Banking Risk Information Centre warned recently.

Read this article on the website Click Here
Striking the balance in data governance

Posted by Norbert Boon on September 13, 2010 at 12:25pm

Despite recent news reports that the Basel III liquidity requirements are to be pared back, financial institutions are still facing vast regulatory challenges. They already have to hold more capital and liquidity, as well as report on this daily. Going forward, institutions will also have to demonstrate the processes and controls used to put together reliable information. Never before have risk and data management been so interwoven.

The real challenges facing institutions looking to showcase their transparency to regulators are the problems that result from siloed business units and manual processes. These can result in institutions not being able to determine a good instrument price from a bad one, or even tell who issued the instrument in the first place. If they can’t do that then they certainly can’t demonstrate independent pricing. Furthermore, data management often falls under the responsibility of IT. However, all too often the IT department doesn’t have the specific front and middle office insight needed to ensure that data is managed according to business requirements.
Let’s not forget what’s at stake if data governance fails – sure, the fines can be large, but it’s the increased capital margins entailed in not being able to demonstrate compliance that really hurt. Also, throwing money at the issue and massively boosting compliance costs is not necessarily an option at a time when budgets are so severely limited.

So what’s the solution? Institutions need to take a business process-led approach to data governance, based on the principles of independence and transparency. Incorporating business rules into data management is a must. These rules or service level agreements will be specific to the bank – such as guaranteed delivery times of prices from specific countries. Right now, most banks haven’t yet joined this up to the data management process, which is what makes it so difficult to determine what went wrong or gain an early warning of potential issues. As a result, what could have been addressed as a small discrepancy often snowballs into a big problem.

Equally important is being able to draw up a full audit trail of the data. This should not only show exactly where the data has come from, but must also provide real-time information about all data events, such as errors, new product take-ons and model updates. Continuous monitoring for data governance of the whole, and
preferably centralised, process is also paramount. In taking this measure, banks will achieve better compliance and drive down operational risk by giving business users unparalleled transparency.

These best practices – particularly if conducted across price, reference, counterparty and corporate actions data – are key to mastering the compliance and competitive balancing act. If institutions act now and get this right, they will not only comply with these increasingly stringent regulations, but also reduce their risk and capital overhead.

Read this article on the website Click Here
ERM: 5 Steps to Success

Most agree that working from the top down, meaning to first identify corporate objectives, then focus on the details of how to achieve them is what most managers wish they could be doing more of. However, the reality is most managers are so busy with day-to-day activities that little time is left over to work on the big picture. Everyone agrees the role of ERM is for risk management to be involved in the “key business decisions,” however, some misinterpret this as interviewing only the senior executives in “big picture” assessments. In reality, aligning day-to-day activities of all managers to the strategic objectives set senior leadership, and then aggregating and analyzing this information is the winning approach.

So how is this accomplished?

Here are the 5 steps to quickly and practically embed risk management enterprise-wide.
1. Begin with a "quick win"
Day-to-day activities are managed by business process owners throughout the organization. Winning the hearts and minds of these managers is all about helping them get current and in control of what’s in their “inbox”. Being in control of their current work will free up needed time and energy to understand and contribute to the “big picture.” Start with a business function that your direct boss is already responsible for, such as vendor management, information security, fraud, internal audit, regulatory compliance or business continuity. Your boss is highly motivated to get things done and has the resources, expertise and authority to help you make a “quick win” with this business area in less than 90 days. Quick wins build confidence, skills and attract other managers to seek you out and invite you into their world.

2. Streamline current daily activities
An organizational system is needed to reach managers and help them connect to the big picture. A successful system will immediately streamline their daily tasks so nothing falls through the cracks. This organizational system is called “ERM Software.” Often, I have been asked for real world examples of this technology successfully adopted. Believe it or not, one of the best examples of a risk-based approach is Facebook or
LinkedIn. Consider the task of documenting and connecting every person on Facebook, “the big picture,” from the top down in spreadsheets. This approach would be impossible! That is why Facebook instead focuses on the immediate problem of providing an organizational structure that allows users to share their information easily and quickly. Most importantly, the structure automates what each user is attempting to achieve, building a “big picture” network of contacts they can call upon when they need them. ERM Software is real and operates with the same technology and approach, but unlike a "social network", ERM Software builds a “corporate network” of information, updates, and connections fully controlled by your organization. ERM Software grows in value exponentially, like Facebook does, with minimal oversight and expense. This same organizational structure enables you to aggregate and analyze this information to deliver the “big picture” to the board and senior leadership.

3. Make relationships visible
Separation of duties originally focused employees in departments that were structured to manage only one subject, like vendor management or IT security; however, corporate silos have been crumbling, leaving such employees unprepared to meet these new challenges or uncover the inter-dependencies between
their efforts. A risk taxonomy within ERM Software provides a structure to collect the information already in use by your organization. Additionally, like the role of Facebook or LinkedIn, ERM Software does all the heavy lifting: finding who is connected to who, maintaining these relationships on your behalf, and automatically notifying you of changes you should know about. No more “missing the memo” or “gaps” in your control environment. At the click of a button ERM Software uses these relationships to connect a manager’s activities to the leadership team’s strategic objectives. Just like Facebook, these relationships communicate information both vertically and horizontally, resulting in the alignment of activities without any additional work from participants.

4. Use risk assessment tools to prioritize tasks
Stress comes from inappropriately managed commitments. A risk assessment asks the question, ”What is the business impact and should I really make this commitment?” A risk assessment not only helps each manager prioritize tasks, but also covers their backs with sound reasoning using an enterprise-wide evaluation criteria. ERM Software enables managers to make the business case for allocating resources to their
most critical tasks, making work faster and easier to accomplish. A risk assessment score is attributed based on relationships in step 3 to all connected policies, contracts, and controls, automatically prioritizing work and making clear what should be done the next today.

5. Establish the ERM Process
I have discovered that one of the major reasons managers are skeptical about ERM is that they have tried to do all five steps of risk management at the same time and by themselves. ERM Software, like Facebook and LinkedIn, creates step-by-step wizards that organize your thoughts into a system that you can trust and rely upon. ERM Software reminds you when to identify, assess, evaluate, mitigate, or monitor risk and it connects you to those that can help you complete tasks in half the time. Creating an enterprise wide network of assets, processes, and risk at one point seemed impossible, but by empowering users and equipping management with the appropriate structure, it can be accomplished in as little as 90 days.

So what is holding you back from getting started?
Don’t buy any ERM Software at all, just pay-as-you-go with a full spectrum ERM SaaS Cloud service. LogicManager can have you up and running in 5
business days without any upfront hardware or software investments, and no IT work, and no long term commitments—just all the built in content you need, all connected. Hard to believe? Click here to watch a 4 minute video of how to get your first quick win using your data.

Read this article on the website Click Here
Do you agree with the following statement "A poorly designed control that is followed is still better than a well-designed control that's ignored."

How do u approach this question

Read this article on the website [Click Here]
According to a 2011 McAfee report on second quarter threats, there were 12 million unique samples of malware for the first half of the year, up 22 percent over 2010, making 2011 the busiest six months in malware history.

As smartphones are used increasingly for mobile payments, and mobile betting, mobile crime exposes mobile operators to business risks from unauthorized account access, fraud, and financial crime.

“Smartphones are an attractive target for criminals as “there is a lot of money involved, it is an easy job, and it is low risk.”

Eugene Kaspersky, Founder of Kaspersky

Features

38 Mobile Phone Crime and Fraud Risks
38 Cybercrime and Theft Risks
38 Mobile Phone Theft Crime Wave
39 Recycled Mobile Data Risk
39 Mobile Network Vulnerability
40 Subscriber Data Risk
40 Prepaid Mobile Phone Risks
41 Mobile Authentication
42 Cyber Attacks
42 Mobile Cybercrime Risks
44 App Store Risk
44 iOS Vulnerability
45 Android Vulnerability
45 Mobile Security Measures

**Metrics**
48 Mobile Security App Download Survey-August 2011

Available to subscribers, or as a single-issue purchase ($99).

Jacques LeDisco

Mobile Betting News

blackjax777@gmail.com

http://www.amazon.com/dp/B005J044TO

Read this article on the website [Click Here](http://www.amazon.com/dp/B005J044TO)
Japanese Nuclear Crisis: lessons for risk managers

The nuclear crisis still unfolding at Fukushima Daiichi continues to threaten a meltdown as core temperatures and radiation leaks continue to fluctuate. The disaster is one of the worst nuclear disasters in history. However, the vulnerabilities at the power station are not isolated to Japan or utility companies; they are common risk management shortcomings in operational practices seen in every country and every industry. Here are a few lessons for managers from this crisis.

**Link controls to the assets they depend on.**
Managers’ often make the mistake of assessing the effectiveness of a single control without expanding the scope of assessment to the assets that control depends on.

For example, the Fukushima plant had multiple backup cooling systems to prevent a core meltdown. However, they all depended on a single diesel generator and battery backup system. When the system was discovered
to be damaged, battery backup was depleted within hours and the cooling systems were rendered useless.

Managers will have better business results by expanding the scope of risk analysis beyond a control to the systems and assets it depends.

**Evaluate risk impact for each business process.**

It’s very typical for managers to over-invest in risk controls for one area while leaving other areas widely vulnerable. This over-focus on a single area stems from risk analysis ending at the business unit level without considering how each business process will be impacted.

Going back to the plant at Fukushima, while extreme attention had been paid to containing a potential reactor meltdown, the same level of attention was not invested to protect spent fuel. This under-investment in controls for spent fuel pools has lead to highly unstable conditions including radiation leaks and a potential meltdown outside the main containment vessel.

Managers at the business process level have the best knowledge to identify and evaluate the possible impact of a risk. At Fukushima Daiichi that means managers would assess the impact of a natural disaster on for each business process managing fuel storage, cooling systems,
backup generators, all the way down to employee performance; not just the impact on reactors.

According to the RIMS State of ERM Report 98% of organization’s fail to assess risk at the front-line. This is a widespread problem for risk management programs in every sector.

**Routinely revisit risk assumptions to reveal emerging risks.**

While executives recognize the business environment is constantly changing, the State of ERM Report shows 86% of business continuity plans are based on outdated assumptions. This leads to outdated controls whose effectiveness may no longer be valid in the current environment.

For the Japanese nuclear plant this means assessing the increased probability of natural disaster stemming from global climate change and updating models based on the latest geological information. Managers need to regularly revisit risk assumptions to prevent controls from becoming outdated.

**Evaluate risk from vendor relationships.**

Every organization depends on partners to maintain key equipment and provide key services under emergency situations. Yet, according to the RIMS report, 96% of
organizations today do not cover risks from their vendor partners adequately.

Examples are everywhere, whether you look at the BP disaster and it’s outsourced oil rig from Deepwater Horizon or the Japanese nuclear crisis stemming from vulnerabilities in the original GE reactor design.

Managers must evaluate how vendor relationships impact every area of operations and what essential processes may depend on these relationships. While a process or a technology may be outsourced to a vendor, you ultimately own the risk.

Risk management isn’t about trying to predict the future, it’s about being prepared in the right places where it matters most. These practices reveal the relationships between risks and activities within processes, and allow managers to spend less time fixing preventable problems and more time reaching their strategic goals.

Read this article on the website Click Here
Big Data...Big Deal?

Posted by Sebastien Jaouen on October 25, 2012 at 1:00pm

With the recent introduction of recording for voice and SMS on mobile phones for trading activities in the UK, many technologists were raising the issue of “Big Data” as additional voice recording requirements contribute to the growing repository of data being held by their firms to meet with regulator requirements. Although regulators around the globe are driving for greater visibility and a more comprehensive record of past trading activities, this additional data can also serve a purpose in other areas such as dispute resolution.

With Big Data, technologists share the concern that they appear to be facing a rapidly increasing need to hold more data. This is not only a challenge in respect of volume, but also diversity. Trading communication now takes many forms; voice, IM and SMS as well as factoring in social networks, email and other systems related data (i.e. electronic payments or transaction messaging). The expectation is that regulators will push for this broader range of data types to be held for far longer periods than before, with current averages in the range of 3-6 months moving closer to 3-5 years (as seen in Dodd Frank and MiFID II proposals). Planning ahead
for storage requirements is also a challenge, as volume and diversity of data is often affected by increased activity in the markets which is hard to foresee, along with the seasonality of specific market activities. The main concern is that existing data technologies and infrastructures could soon reach their limits of scalability and performance.

So how can these data and analytics hurdles be approached? In today’s cloud based technology “as a service” world, we are seeing institutions seriously considering specialist service suppliers to provide flexible data storage solutions that are fully scalable. Although this was not a strategy that was immediately accepted for critical applications, due to uncertainty on the risks in security and reliability, the general concept of outsourcing key infrastructure (data storage) along with highly proprietary and confidential data is now gaining acceptance.

Overall, this is a situation that is still developing, where the larger the firm the quicker the issue of “Big Data” could become a reality. However, timing could be an issue here as these solutions are still relatively new and need to allay concerns, especially with the cautious and risk adverse solution teams within firms. As a trader, voice challenges around recording requirement for
compliance go beyond the previous areas of expertise of the telecommunication specialists, and clearly demonstrates the impact technology convergence already has in this sector, where lines are far more blurred between technologies deployed and managed across the trade floors.

Read this article on the website Click Here