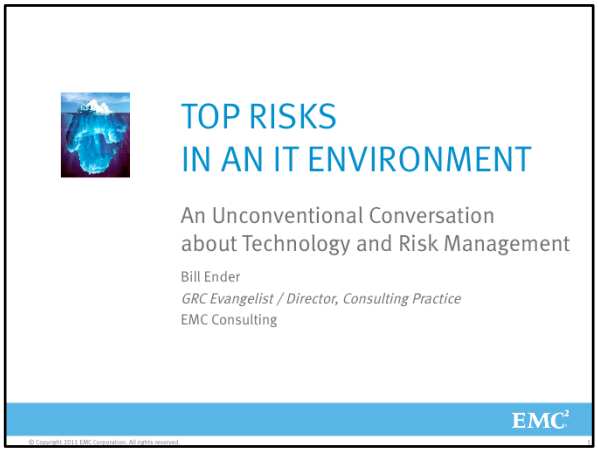
Top Risks in an IT Environment

Bill Ender / EMC Consulting



I'm a GRC guy – as in Governance, Risk and Compliance. I've been out of the day-to-day operations of IT for several years, now, after having lived there for the better part of 20 years. I grew up writing silly little BASIC Plus programs on a Teletype 33 terminal connected to a time-shared DEC PDP11. Like some of you, probably, I thought my TRS-80, then, later, my Osborne "portable," were the coolest things ever invented. And I paid an insane amount of money for the whopping 40MB hard disk drive for my first IBM PC AT – the thing was half the size of a loaf of bread, weighed about five pounds, and cost me close to $1,000 *including* the discount. But enough about my brilliant investment skills. I don't do hardware … or software … any more. In fact, I barely tolerate technology sometimes.

Most of the time, these days, I try to confine myself to evangelizing about GRC. It's a relatively new area – not quite mainstream – but getting a lot of buzz and attention in the boardroom. And even though I've lost some of my lust for new *technology,* I'm a big fan of new movements and ideas – especially things that I view as transformational. GRC is one of those things.

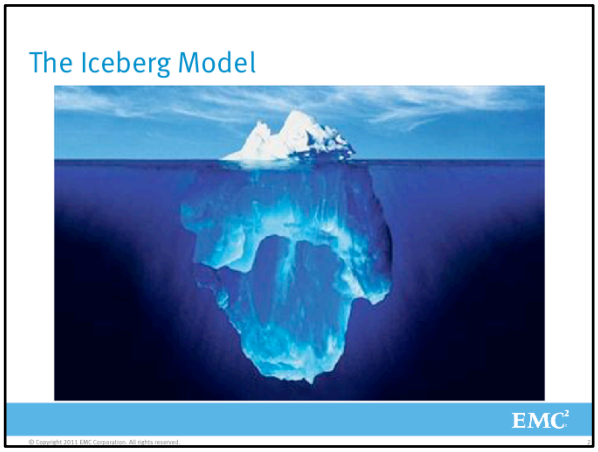
I've been asked to speak to you about "Top Risks in an IT Environment." OK … I can do that. But I'm not going to run through a litany of attack types or highly technical details. You will find no bullet points or "eye charts" here. I'm more of a "big picture" guy. My paintbrush is the 3" or 4" model – broad brush strokes that cover larger expanses … or maybe a roller … the kind of thing you might use to paint the side of a barn. At the end of this hour, we may not have all of the detailed trim work done, but you will have a solid understanding of my view of the barn.

One more note before we get started … the reason I work for EMC Consulting – other than the fact that they let me use the title "GRC Evangelist" on my business card and happily pay my Starbucks bills – is that we share a vision about new ideas and transformation. GRC is one of EMC's top corporate initiatives, along with Cloud Computing and a few others areas in which the company is an acknowledged and respected thought leader. The combination of EMC Consulting with RSA – the Security Division of EMC – VMware, and the other products, services, and partners in EMC's brain trust is my sandbox. And there's nothing I enjoy more than playing in my sandbox and building new things.

[END OF EMC PROMO HERE] &;-)

Top Risks in an IT Environment

Bill Ender / EMC Consulting

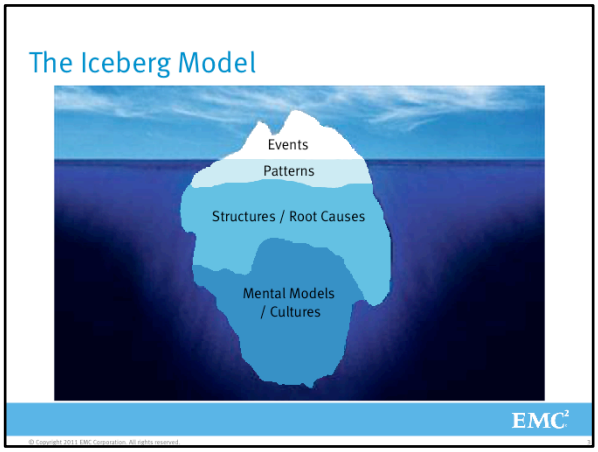


This is what IT risk looks like to me – an iceberg. Coincidentally (or maybe not), this also is a model for an approach to problem solving called "systems thinking." We know that an iceberg has only 10 percent of its total mass above the water while 90 percent of it is underwater. And the shape of the underwater portion can be difficult – if not impossible – to determine by looking at the portion above the surface. In short, what you see is only a small part of the total; there's a lot more under the surface and and its appearance and effect on the visible portion might surprise you.

*Adapted from *It's All Connected: A Comprehensive Guide to Global Issues and Sustainable Solutions,* by Benjamin Wheeler, Gilda Wheeler and Wendy Church. www.facingthefuture.org

Top Risks in an IT Environment

Bill Ender / EMC Consulting



If we apply the iceberg model to IT risks, we could say that at the tip, above the water, are *events,* or things that we see or hear about such as network attacks, information and equipment thefts and losses, viruses, fraud, etc. Most of our time is spent at the events level as we go about our daily business. But because events only represent the tip of the iceberg, if we look at IT risks only at this level, we tend to be reactive and driven toward short-term solutions.

If we look just below the water line, we often start to see *patterns.* Patterns are changes in variables over time. Within the context of IT risk, think of viruses that mutate and recur over time … or spam. If you receive a piece of email from someone you don't know, that could be a singular event; if you receive the same email from several different sources over a certain time interval or if a large number of people you know or work with receive the same email message, that's a *pattern*. Recognizing patterns allows us to anticipate, plan for and forecast risks – to adapt so that we can manage risk more effectively.

Like the different levels of an iceberg, beneath the patterns are the underlying *structures or root causes* that create or drive those patterns. For example, the underlying structure of problems such as information losses might be our failure to properly classify information or failure to enforce policy regarding information use. If you look only at the event, you might think that we should just deploy additional technology or controls to defend against network attacks. But looking deeper into the structure of the problem might suggest automating information classification and policy enforcement as a means to reduce the risk of information loss.

Finally, at the base of the iceberg are the *mental models* or *cultures* that create or sustain the structures above. If the culture of a business is, "corporate policies are too restrictive," line of business executives might be more inclined to develop independent approaches to policy development, risk management, and incident response. If the culture is, "we are one company," executives might be more amenable to centralizing common functions and developing a more coordinated, role-based method of operation. The important thing to understand is that in solving problems, the greatest leverage is in changing the structure – applying deep ocean currents to move the iceberg, which will change the events at its tip.

An example of the iceberg model can be seen in mobile device thefts and losses. The theft or loss of a smartphone or laptop is an event; an increase in data breaches associated with mobile devices is a pattern. The systemic structures or causes of data breaches associated with mobile devices might include lack of policy or training regarding mobile device use, weak or no policy enforcement, or improper classification and/or protection of information. We tend to get lost in the immediate event of the loss, forgetting that it is part of a pattern of events that is caused by the underlying structures of our business environments. If we take a systems thinking approach to solving the problem of mobile device thefts and losses, we might try to find ways to automate policy enforcement or reduce exposure of sensitive information, rather than just focusing on the immediate relief (e.g., prohibiting the use of mobile devices) that addresses the most recent event.

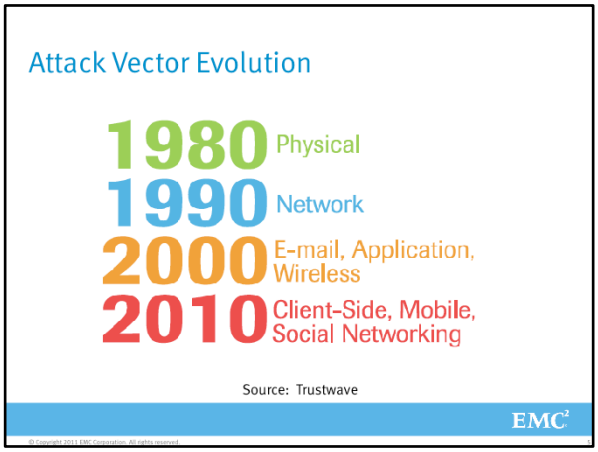
Top Risks in an IT Environment

Bill Ender / EMC Consulting

There are a lot of other reputable sources for detailed information about reigning IT risks and best practices. Several of the sources represented here I will reference later in our conversation; and you'll find links to them within the Notes accompanying this presentation – a copy of which you all will receive.

General IT Security Risks

1. Criminal attacks
2. Weaknesses in infrastructure
3. Tougher statutory environment
4. Pressures on offshoring / outsourcing
5. Eroding network boundaries
6. Mobile malware
7. Vulnerabilities of Web 2.0
8. Incidents of espionage
9. Insecure user-driven development
10. Changing cultures



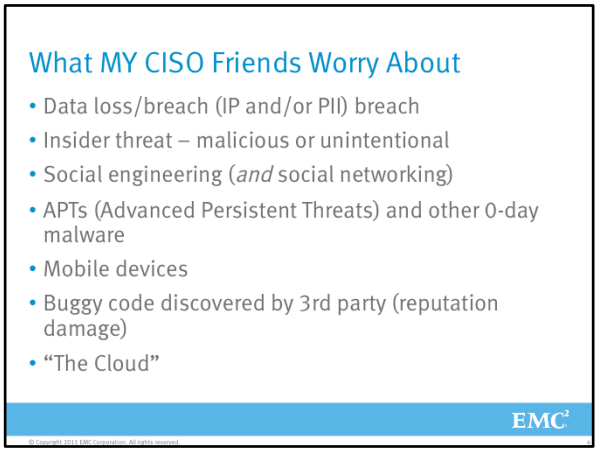
Until 2010, the majority of all data breaches were perpetrated via one of five vectors: physical, network, e-mail, application and wireless — all five of which have been used in varying degrees over the last three decades. As the availability of bandwidth to people all over the world has increased over the last decade, so has the richness of the content and applications utilizing these networks. When complexity is added to any client-side application, browser or viewer, the potential for exploits increases.

As we have moved away from desktops and laptops to mobile devices and tablets, many of the security principles developed and enforced over the last two decades appear to be declining in importance. Concerns about privacy, once pervasively guarded, seem to be decreasing with the advent of social media tools. Just as the "open source" movement has transformed the landscape of application development, so the new "open access" social networking environment has changed the ways in which we communicate and interact with one another, as well as the tools we use. Intent on accessing private data, the emerging attack vectors for the 2010 decade are none other than client-side, mobile and social networking.

Trustwave *Global Security Report 2011:*
https://www.trustwave.com/downloads/Trustwave_WP_Global_Security_Report_2011.pdf

Top Risks in an IT Environment

Bill Ender / EMC Consulting



OK … I promised no bullet points. But just this once. *Honestly,* there are no more (I just peeked ahead)!

Here are some of the most frequently noted IT risks about which my CISO and CIO friends are concerned. These aren't listed in order of importance or threat level, because those ratings vary somewhat, depending on industry sector and individual. However, suffice it to say that almost *all* of them acknowledge that the primary risk underlying all of these is ‹drum roll› information theft or loss ‹cymbal crash›.

We'll explore a few of these in more detail – a couple, in particular, that most, including me, agree represent the overwhelming majority of IT risk these days and for at least the next couple of years.

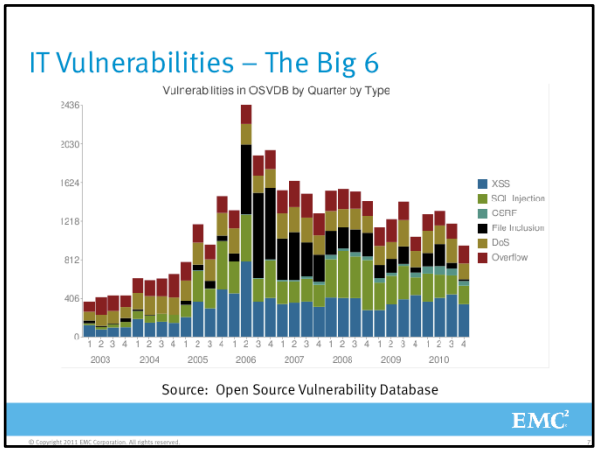
And though I mention "The Cloud" – which is an area of increasing importance – I confess, I *will not* get into details in this area. This is because 1.) There are several other people among my colleagues who are much better informed than I am about that topic and 2.) We easily could spend an entire day on "cloud" alone.

I will, however, take a moment, here, to talk a bit about Advanced Persistent Threats, which have been in the news lately.

[DISCUSSION RE: RSA AND GOOGLE APT ATTACKS HERE …]

Top Risks in an IT Environment

Bill Ender / EMC Consulting



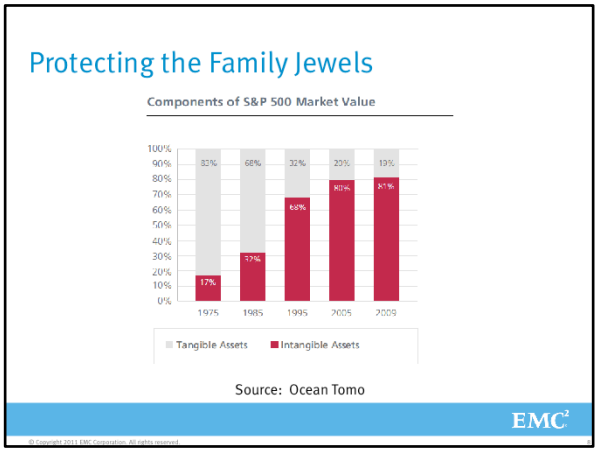
The top half-dozen conventional IT *technology* risks have maintained a fairly consistent profile over the past decade. Though, their ranking within the broader spectrum of IT risk has declined somewhat over the past several years.

<u>OWASP (Open Web Application Security Project) Top 10 Web Application Security Risks for 2010</u>

A1: Injection
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object References
A5: Cross-Site Request Forgery (CSRF)
A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards

Open Source Vulnerability Database:
http://osvdb.org/

OWASP (Open Web Application Security Project) Top 10 Web Application Security Risks for 2010:
http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project



In my opinion, the much more significant trend influencing IT risk arises from a transformation that has occurred at the macro level of commerce and the global economy.

Over the last 35 years, the majority of the developed world has evolved from a manufacturing economy to an information economy. Through most of the first three-quarters of the 20th century, the overwhelming share of an organization's value centered on its tangible assets. Manufacturing was king – propelled by mid-century advancements in automation and distribution. Intellectual property (IP) certainly had value; but getting at IP – negotiating the physical and social barriers protecting it – was challenging and time-consuming. In the last 15 to 20 years, as a large percentage of global manufacturing has moved "offshore," we have witnessed a major shift in market valuation from tangible to intangible assets. Intangible assets – *information* – once representing barely one-fifth of market valuation now comprise more than four-fifths of market valuation among global business leaders.

Kroll Global Fraud Report

-In 2010, Information Theft/Loss/.Attack (32%) surpassed Theft of Physical Assets/Stock (27%) as most common form of fraud for first time in history
- 87% of companies report experiencing fraud
- Fraud is most often an inside job (44%)

Open Security Foundation Data Loss DB

Breaches 2010
- Total Incidents: 451
- Total Records Affected: 27,972,020

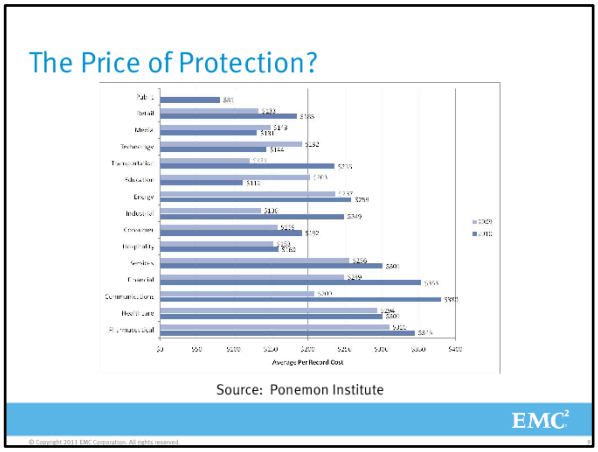
Breaches 2011 YTD
-Total Incidents: 97
-Total Records Affected: 5,264,960

Kroll *Global Fraud Report Annual Edition 2010/2011:*
http://www.kroll.com/library/fraud/FraudReport_English-US_Oct10.pdf

Open Security Foundation Data Loss DB:
http://datalossdb.org/

Top Risks in an IT Environment

Bill Ender / EMC Consulting



IT budgets, as a percentage of overall budgets have increased, of course; but like electricity, IT has become a cost of doing business in the modern world – if you're in business, you're going to spend money on IT. With information playing a central role to most businesses, the cost of securing information has assumed greater importance and, as a result, consumed a larger portion of IT budgets. It should come as little surprise, then, that the cost of recovering from information thefts or losses has increased.

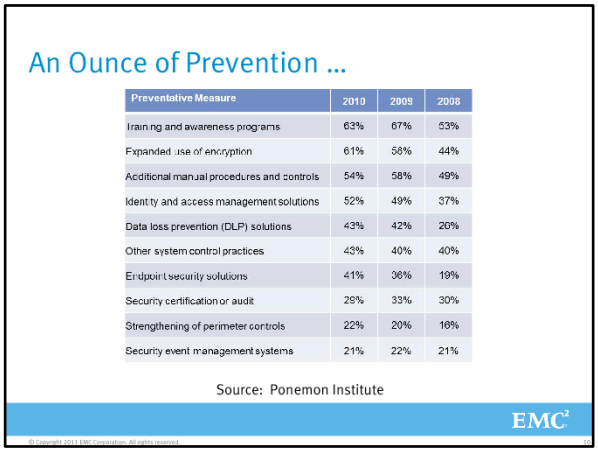
Ponemon Institute

- Average cost per customer record: $214
- Average organizational cost of a data breach: $7,241,899

Ponemon Institute *2010 Annual Study: U.S. Cost of a Data Breach:*
http://www.ponemon.org/news-2/23

Top Risks in an IT Environment

Bill Ender / EMC Consulting



Preventative Measure	2010	2009	2008
Training and awareness programs	63%	67%	53%
Expanded use of encryption	61%	56%	44%
Additional manual procedures and controls	54%	58%	49%
Identity and access management solutions	52%	49%	37%
Data loss prevention (DLP) solutions	43%	42%	26%
Other system control practices	43%	40%	40%
Endpoint security solutions	41%	36%	19%
Security certification or audit	29%	33%	30%
Strengthening of perimeter controls	22%	20%	16%
Security event management systems	21%	22%	21%

Tools and technology may help reduce the risk of information theft and loss, but the underlying *structures* and *mental models* within an organization (remember our iceberg?) play a central role in reducing this and other IT risks. An increasing number of organizations view risk mitigation via increased emphasis on Training and Awareness, *in combination with* tools and technology, as the "ounce of prevention" that could result in the "pound of cure" for information security.

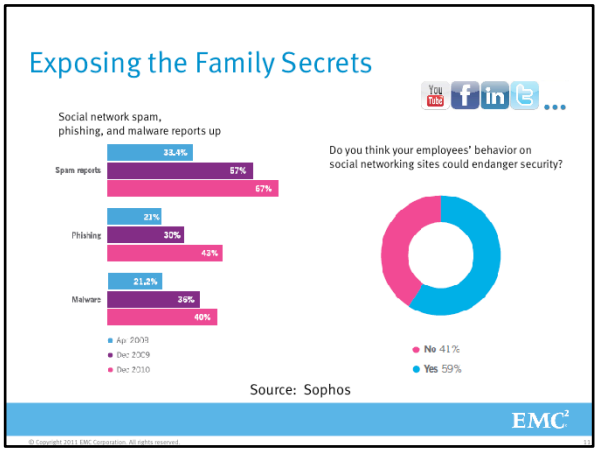
Ponemon Institute

- Training and awareness programs remain the most popular post-breach remedies, but encryption and other technologies are gaining fast
- Companies continue to rely on educating their workforce and enabling it to personally help stop future data breaches
- Companies are increasingly aware of, and willing to implement, technology solutions to help prevent and mitigate breaches

Ponemon Institute *2010 Annual Study: U.S. Cost of a Data Breach:*
http://www.ponemon.org/news-2/23

Top Risks in an IT Environment

Bill Ender / EMC Consulting



A study published in 2010 entitled "Employer Perspectives on Social Networking" that compiled data from 34,000 businesses in 35 countries surfaced a startling statistic: "75% of employers say their business has no formal policy instructing employees on the appropriate use of social networking sites on the job." Yet, spam, phishing (in all forms), and malware spawned from social network vectors has increased at an exponential rate. Over 90% of organizations today allow access to social networking venues and utilities such as YouTube, Facebook, LinkedIn, Twitter, and others.

The ubiquity of social network use and its increased penetration of corporate boundaries is reflected in the growth of the three largest social networking venues:

- LinkedIn took almost 10 years to reach 100MM users (Mar-2011)
- Facebook reached 200MM users in 5 years and 2 months (610MM as of Feb-2011)
- Twitter grew from 75MM users in Jan-2010 to 200MM users in Jan-2011 (over 100% faster than Facebook over the same period)

The convergence of social networking with mobile device use represents, in my opinion, *the* most significant and challenging IT risk to date.

Risks of social networking to business include

- Vulnerability of IT infrastructure from malicious software downloaded from social networks
- Involuntary disclosure of sensitive business information
- Negative or unfair criticisms in a public arena that rivals could use to their advantage

Question: Does anyone know what "clickjacking" and "likejacking" are?

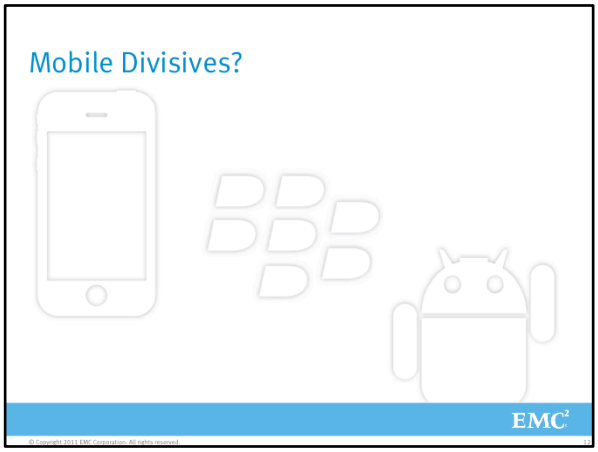
Best practices

"The Rules of Social Media Engagement," by Brian Solis:
http://www.briansolis.com/2011/03/the-rules-of-social-media-engagement/

Sophos *Security Threat Report 2011*:
http://www.sophos.com/security/topic/security-threat-report-2011.html

Top Risks in an IT Environment

Bill Ender / EMC Consulting



From the early ’80s to the mid-’90s, cell phones were popular targets for fraud and cloning due to inherent weaknesses in the cellular network architecture. As mobile networks migrated to GSM and CDMA technology, these vulnerabilities decreased significantly; though CDMA cloning is still possible, GSM cloning attacks are very difficult. In addition, wireless service providers have become much more vigilant about detection and deterrence. But while the threat of device cloning has decreased, the overall risk profile of mobile devices has increased dramatically.

Mobile device technology advancements of the last decade have led to always-connected, Internet-enabled phones and other devices. At the beginning of 2010, around 500 million devices existed on 3G-enabled networks. A typical smartphone today has the same processing power as a PC from 8 years ago, but also supports an array of advanced hardware capabilities such as built-in audio, video and geographical location. With the advent of 4G network technology and the continued acceleration of hardware and software capabilities, today’s most sophisticated mobile devices will be ghosts in 3 to 5 years.

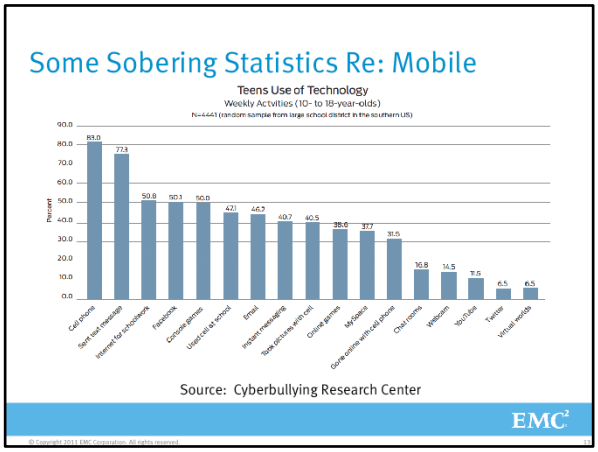
Yet, while advances in performance, storage, and capabilities of mobile devices continues to accelerate, security remains a virtual greenfield.

Loss and Theft of Mobile Devices

- No longer need to possess actual device to compromise it

Communication Interception

- Can monitor SMS and MMS messages, emails, inbound/outbound call logs, and user locations
- Can even allow an attacker to remotely listen to phone conversations
- Near-Field Communications (NFC) exploits already appearing



Cell phones continue to be the most popular technology used by adolescents, with almost 83% of youth having used one at least weekly according to a 2010 study by the Cyberbullying Research Center. Other research published by Nielsen and the Pew Internet Project indicates that 33% – 35% of U.S. youth *and* adults have smartphones with advanced data features.

Gartner analysts forecast app downloads from mobile device application stores (e.g., Apple App Store, RIM BlackBerry App World, Android Market, Handango, etc.) to reach 17.7BB in 2011 – a 117% increase from an estimated 8.2BB downloads in 2010. By the end of 2014, Gartner forecasts over 185BB applications will have been downloaded from mobile app stores since the launch of the first store in July 2008.

Malware – 250% increase 2009-2010

- Trojans that send SMS messages to premium-rate numbers
- Background calling applications that rack up exorbitant long-distance bills for victims
- Keylogging applications that can compromise passwords
- Self-propagating code that infects devices and spreads to additional devices listed in the address book
- Polymorphic attacks (malware that changes characteristics during propagation to avoid detection)
- Spyware that monitors device communications and can be remotely controlled by cyber criminals
- Commercial spyware applications — e.g., FlexiSpy (www.flexispy.com), Mobile Spy (www.mobile-spy.com), and MobiStealth (www.mobistealth.com) — are readily available and effective at concealing their presence from the user of an infected device

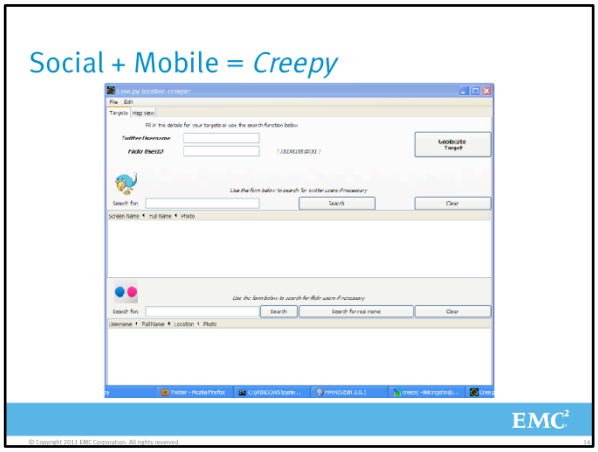
Cyberbullying Research Center:
http://www.cyberbullying.us/research.php

Juniper Networks *Mobile Device Security – Emerging Threats, Essential Strategies:*
http://www.juniper.net/us/en/local/pdf/whitepapers/2000372-en.pdf

Gartner Worldwide Mobile Application Store Revenue Forecast:
http://www.gartner.com/it/page.jsp?id=1529214

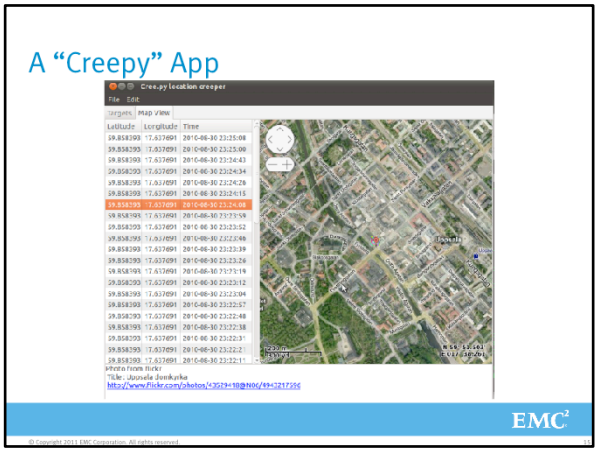
Top Risks in an IT Environment

Bill Ender / EMC Consulting



One of the latest open-sourced tools being used to exploit unprotected data generated by the convergence of mobile devices and social networking platforms is this application, rather appropriately named *Creepy.*

Input a Twitter or Flickr username and click the **Geolocate Target** button …



… and up pops a detailed listing of date/time-stamped latitude/longitude coordinates of that Twitter/Flickr user's movements, based on GPS data generated by their mobile device(s). This can be (and *is* being) used by curious teens and professional hackers to capture information from unsuspecting mobile device/social media users. "Creepy" is available on Windows and UNIX platforms today; and the source code is freely downloadable from a wide assortment of servers across the Internet.

Think about that the next time you tweet or take a photo with your smartphone. Is your phone configured to capture your geocoordinates … do you really want it to do that?

This is only the *beginning* of what we will see in the way of social/mobile "mashups" in the coming months/years.

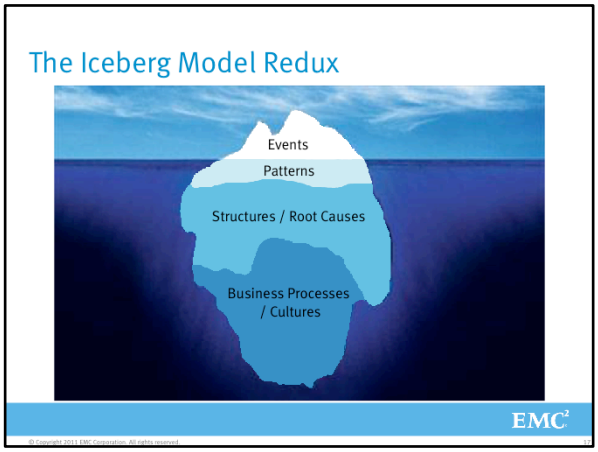
Top Risks in an IT Environment

Bill Ender / EMC Consulting

I know what you're thinking: This might be the only secure place to be in the world, today (but probably not).

Top Risks in an IT Environment

Bill Ender / EMC Consulting



Events happen. And they will continue to happen regardless of what we do. For every problem we solve, every defense we put into place, some new thing will pop up to take its place in the risk portfolio. As technology continues to evolve and our society and the way we interact with one another continues to change, risk vectors will become more complex and sophisticated. What we invent today to defend information and infrastructure eventually will be exploited to compromise it.

Isolated events will happen occasionally. But *look for patterns:*

- Things that happen regularly in a particular business unit
- Breaches that occur across multiple business units or geographic regions
- Similar breaches within a particular industry sector (Open Security Foundation Data Loss DB, Open Source Vulnerability DB are reliable sources)

If you see a pattern, there's likely a *structural* issue or *root cause* driving it. Problem: Laptop encryption rollout leads to false sense of security, which leads to increased laptop thefts. **Solution:** Increased Training and Awareness campaign focused on laptop security leads to better understanding or *reputation* risk, which leads to reduction of laptop thefts

Every structure has a foundation – a *business process* or *culture* that supports it.

- A strong Governance, Risk and Compliance program can help to identify common interests, eliminate duplication of effort, reduce complexity, improve efficiency, and increase ROI for IT investments.
- There's no sense in having a policy if everyone in the company is allowed to maintain their own version – that's both a practical problem and a regulatory nightmare waiting to happen. But a well-designed and -implemented exception process can provide flexibility *and* improve visibility of potential risk.
- There are lots of standards and risk management frameworks out there – COSO, CoBIT, ITIL, ISO, OCEG, CAMM* – use them.

* Common Assurance Maturity Model (for Vendor Management)

Top Risks in an IT Environment

Bill Ender / EMC Consulting

Here's the salient information about me and what I'm doing over the next couple of months. Feel free to contact me – or any of my colleagues at EMC Consulting or RSA/Archer (they're skulking around here somewhere) – if you'd like more information about any of this. And remember that GRC, Security and Risk Management, and "The Cloud" is where we live (well … not *literally* … though, I've occasionally been known to get my head stuck there).

I'm not a frequent Twitter user – you won't learn anything about my breakfast or my shopping habits by following me; but I *do,* on occasion, tweet interesting or useful information on GRC-related topics.

However, I am an unabashed and shameless promoter of my colleague, Yo Delmar's, *GRC and Beyond* blog. Yo *knows.* Read her … and tweet her at @YoDelmar.

And though the third rider in EMC's 3GRC Musketeers, Bob Dell Isola, doesn't have a blog and would rather stick needles in his eyes than use his Twitter account (@bdellisola), I encourage you all to follow him – he's "wicked smaht" … and if enough people start bothering him, maybe he'll actually post something sometime.

Top Risks in an IT Environment

Bill Ender / EMC Consulting