

I Don't Know



con-TIN-gen-ZEE: An Information Assurance company that improves security, survivability and profitability by using a low cost, modern methodology.

Presented by
Michael Miora, CISSP-ISSMP, FBCI
Montana Computer Network
Security Conference
9 March 2006

Contingenz
Corporation™

227 Fowling Street, Playa del Rey, CA 90293
www.contingenz.com ▪ info@contingenz.com
310 306 0166 ▪ 310 306 1612 fax

Confession...

- I am a consultant ...
- The Consultant's 12-Step Program
 - In my day job, as a consultant, I visit companies
 - At the start, I know nothing about their operations.
 - Knowing it – admitting it – addressing it – are critical to protect Information appropriately



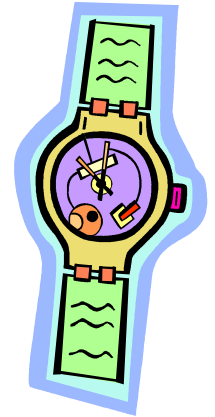
The Consultant

- **Definition:**

- A consultant is someone who borrows your watch to tell you the time.

- **If you have a watch but cannot tell time, then this is an important function to you**

- OK Consultant: Tells you the time
- Better Consultant: Learns why you need to know the time and helps you tell time for yourself
- Excellent Consultant: Helps mold the business processes to make best use of known time



The Consultant Revisited

- **Definition:**
 - An InfoSec consultant is someone who uses your “systems” to improve your security
- **If you have “systems” but don’t know how to make them secure, then this is important**
 - OK Consultant: Makes you secure
 - Better Consultant: Learns what needs to be secured and why to help you put into place processes so you can maintain your own security
 - Excellent Consultant: Helps mold the business processes to make you as secure as you need to be

The Three Secrets

- **Secret 1**

- All Information Assurance (InfoSec, Security, ...) specialists are consultants – be they internal employees or outside consultants

- **Secret 2**

- As a technical expert, you know nothing about your employer's business
- Everyone will question what you do as though they were the technical experts

- **Secret 3**

- If you do your job right, then when you are done, everyone will know they didn't need you
- Remember Y2K?

Secret 1

- **InfoSec specialists are consultants**
 - Employment status doesn't matter
- **Executive meetings include**
 - Sales, marketing, finance, product/service mgt ...
 - Sometimes a CIO
 - Seldom a CISO
- **Learn about new products or services only when technology comes into play**
 - Seldom asked in advance except about technology
 - After the “real” decision has already been made
 - Because “we don't know” the business

Secret 2

- **As a technical expert, you (are expected to) know nothing about your employer's business**
 - Business model
 - Business practices
 - Finances
 - Full range of products/services and why they are designed as they are
- **Everyone will question what you do as though they were the technical experts**
 - Why do we need this or that security restriction?
 - WLAN, Authentication, Encryption, Access Controls, ...

Secret 3

- **If you do your job right, then everyone will know they didn't need you**
 - Remember Y2K?
 - In the absence of a breach, we don't need security
 - After a breach, we complain about lack of security
 - When something happens, Incident Response must be quick, efficient, effective, and “spontaneous”
 - But nobody has time for advance planning
- **Because we don't know the next issue ...**

I Build Plans

- Incident Response
- Business Continuity
- Emergency Response
- CERT – SIRT – CSIRT – ERT ...
- In each case, we plan based on guesses
 - We don't know what will happen
 - We plan for the “unknown”
 - We plan for categories of possible occurrences
 - We hope for the best
- What are we planning for?
 - “I don't know”



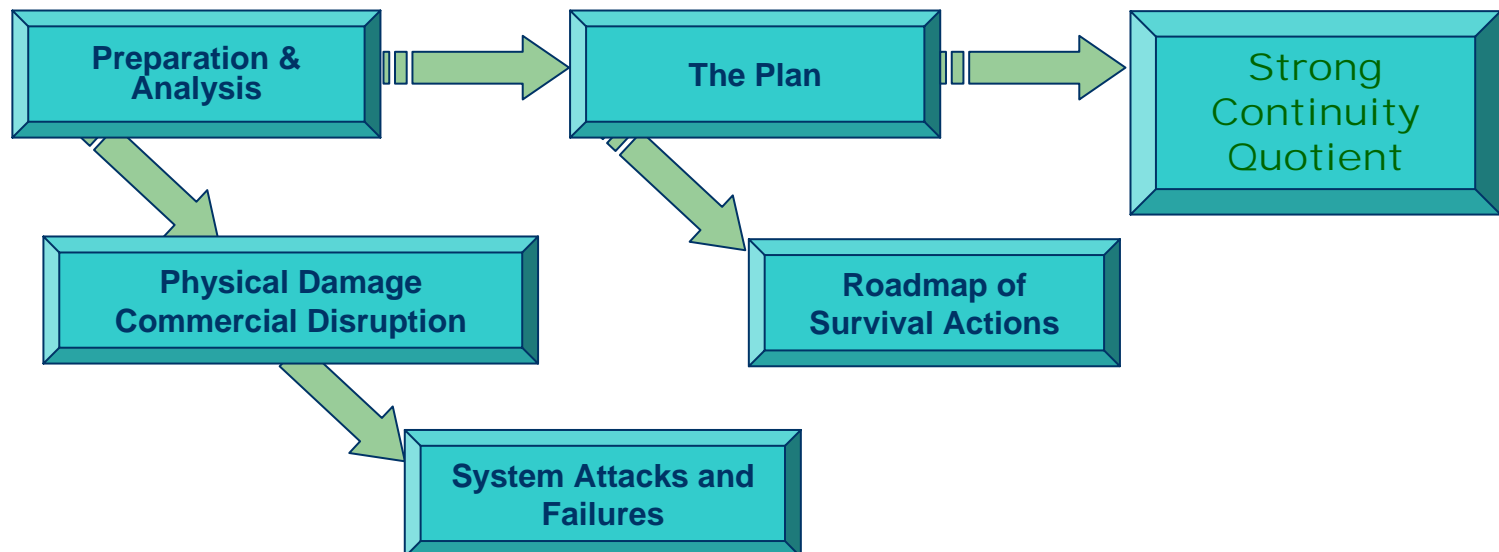
Response Plans: Planning for What?

- **An Example of BC Plans**
- **Everyone talks about Business Continuity Planning as planning to continue business operations**
 - An untrue tautology? What are we missing?
- **Many companies are unprepared ... why?**
 - Isn't it obvious that protection is required?
 - Why isn't it done?
- **Why the “subtle” distinctions between Business Continuity (BC) and Disaster Recovery (DR) and CERT – SIRT – CSIRT – ERT ?**
 - Is the definition covering up a lack of knowledge?
 - (“I Don't Know”)



Defining BC/DR/CERT/SIRT/CSIRT

- **Taking the punch and staying in the game...**
 - The ability of the business to continue generating revenue in the face of significant disruptive events (SDE).
 - Continuity is the payoff of good, solid planning
- **Measured as a *Continuity Quotient*: The ability to withstand SDEs**
 - BC/DR/CERT/SIRT/CSIRT



Analyst Vision

- **Analysts report stark findings**
 - Widespread lack of preparedness among all sized businesses
 - Danger of significant loss of revenue or business closure
 - Recognition of need is growing fast
- **Products in the marketplace**
 - Low cost products are ineffective
 - Other products are too expensive
 - Substantiated need for an effective low cost solution
- **Why?**
 - Perhaps the marketplace doesn't really know it is possible?
 - Or perhaps those providing the solutions don't know the language of business?

Analyst Words of Wisdom

- **Gartner**

- **“Two out of five enterprises that experience a disaster will go out of business within five years ... [unless] they take the necessary measures before and after the disaster.”**
(Aftermath: Disaster Recovery, Gartner, September 2001)

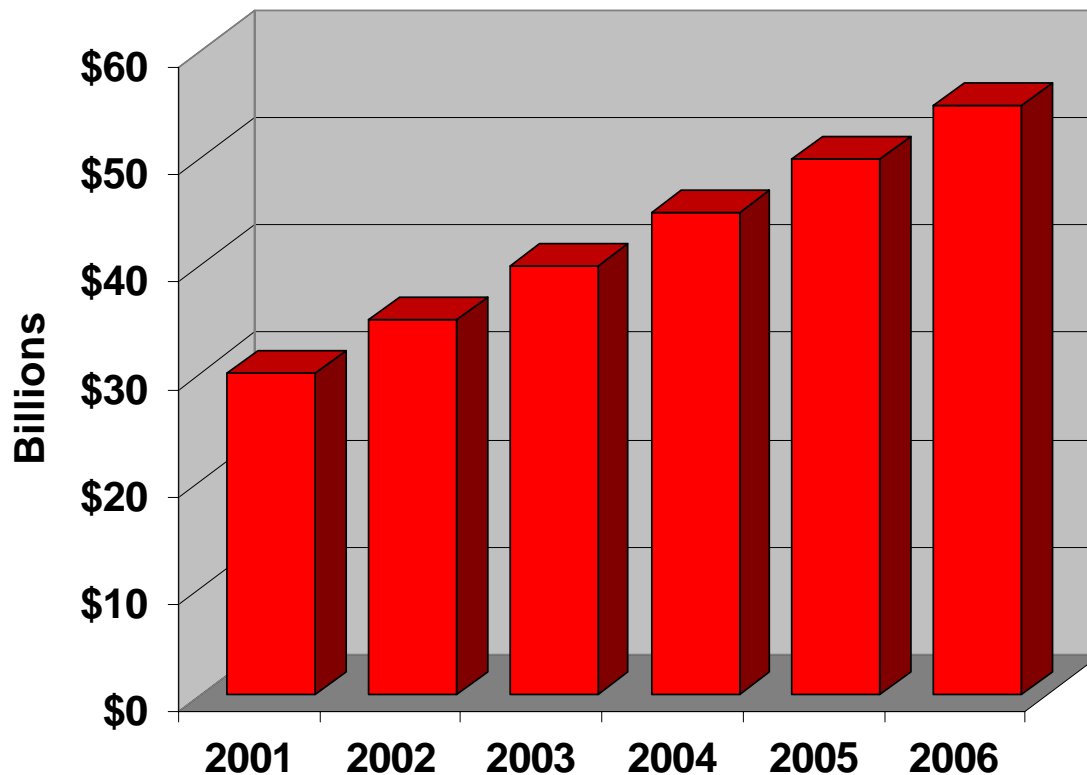
- **“Business continuity planning has evolved beyond ... disaster recovery to include ... business process resilience.”**
(Doc 117614, 30 September 2003)

- **Robert Half Management Resources**

- **37% of CFOs identified preparedness/recovery as their most vulnerable area**
[Management Survey, 2004. Includes responses from 1,400 CFOs from a stratified random sample of U.S. companies with more than 20 employees]

The Market By The Numbers ...

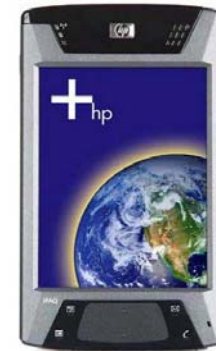
- Market for Incident Management software, hardware and follow-on consulting services business



Source: IDC, April 2003

The Changes – An Overview

- Who builds the plan? Technologists ...
- Who and what do the people do?
- Don't talk about business; Talk business ...
- Requirements, Desirements and the “Gee-Whiz” Factor – Technology and the process
 - What do we need and when do we need it?
 - How do we get it and how soon is soon enough?
 - What is the timeframe?



Plan Generation Step 1

- **Collect information about people**
 - Logistical information
 - Name & Title
 - Address, Phone & Email, Etc.
 - Emergency Services
 - Emergency Sites and Capabilities
 - Key Responders
 - Business Function Information
 - Business functions affected
 - Operational functions supported
 - This is where you “Talk Business”
- **Link all information to business functions**
- **Where is the technology?**
- **Are the technologists the right people to do this?**
- **Perhaps we InfoSec/IA specialists can use this as an opportunity to know**

Plan Generation Step 2

- **Collect information about how the business functions**
 - Perform Business Impact Analysis (BIA)
 - Analyze roles of people, information and equipment
 - Collect information about
 - Key vendors, key customers, outsource providers, critical records
 - Identify key industry-specific issues
 - Correlate to people, information and equipment
- **Link all information to business functions**
- **Where is the technology?**
- **Are the technologists the right people to do this?**
- **Perhaps we InfoSec/IA specialists can use this as an opportunity to know**

Plan Generation Step 3

- **Collect information about technology**
 - Generate inventories
 - Software
 - Hardware
 - Data & Information
 - Describe other technologies
 - Internet, Communications
 - Others
- **Here is the technology**
- **Link all items to business functions**
- **Are the technologists the right people to do this?**
- **Perhaps we InfoSec/IA specialists can use this as an opportunity to show we know by speaking the language of business**

Plan Generation Step 4

- **Document the Plan**
 - Table of Contents
 - Mission Statement
 - Include a Gap Analysis
 - Specific Recovery Procedures
 - Activation Contact List in activation order
 - Various Policy Statements and Guidelines
 - Emergency Services List
 - Activation Steps
 - Regular Procedures
 - Plan Maintenance Instructions
 - Information Sheets
- **Train all business function personnel in more than just the technology**
- **Are the technologists the right people to do this?**

Changing the View – The Language

- **Change the jargon to the language of business – ask if you don't know**
 - Customer Service & Loyalty
 - Revenue
 - Profit & Profitability
 - Share Value
 - Due Diligence
 - Laws, Regulations & Best Practices
- **“Staying in Business”**
 - Continue the Business, not the technology

Changing the View – The Context

- **Support the Business Functions**
 - *People* are your primary business movers
 - *Information* is not just data
 - *Equipment* is not just computers and communication
- **Frame the Problem**
 - **No:** If this system goes down, it will have implications of this and that.
 - **Yes:** What if you could not “fill-in-the-blank”
 - Ask if you don’t know

Other Topics

- **Foundations**

- Computer Crime and Information Warfare
- Penetration, Malware & Other Attacks
- Cyberspace Law & Computer Forensics
- Intellectual Property
- Cryptography

- **Defense, Detection, Mitigation and Response**

- Threats and protections
- Network Management
- Perimeter controls
- E-commerce & Security standards
- Piracy, awareness and ethics
- Business continuity and disaster recovery planning, CERT
- Standards and laws: ISO17799, GLB, SOX and HIPAA

Conclusion

- The next time somebody asks you the time
- Remember to say
- “I don’t know”
- Perhaps you can borrow a watch?



Thank You

***Contingenz
Corporation™***

227 Fowling Street, Playa del Rey, CA 90293
www.contingenz.com ▪ info@contingenz.com
310 306 0166 ▪ 310 306 1612 fax

Michael Miora, CISSP-ISSMP, FBCI
President and Founder
mmiora@contingenz.com
310 306 0111