



# **The Future of Information Assurance**

---

*Techniques to Build Trust by Managing Risks*

Prepared for

Norwich University, MSIA  
Seminar Four: Detection, Response & Hot Topics  
Final Essay

*Report prepared by:*

Becki True, CISSP  
[becki@beckitrue.com](mailto:becki@beckitrue.com)

# Table of Contents

---

<b>TRUST</b>	<b>3</b>
<b>The Heartland Payment Systems Breach</b>	<b>4</b>
<b>VULNERABILITY ASSESSMENT AND INTRUSION DETECTION</b>	<b>5</b>
<b>Software Vulnerability Assessment</b>	<b>6</b>
<b>The Future of VAS and IDS</b>	<b>6</b>
<b>SECURITY POLICIES AND LAWS</b>	<b>7</b>
<b>Censorship and Privacy in the Workplace</b>	<b>8</b>
<b>The Future of Security Policies and Laws</b>	<b>9</b>
<b>RISK ANALYSIS AND RISK MANAGEMENT</b>	<b>10</b>
<b>The Future of Risk Analysis and Risk Management</b>	<b>11</b>
<b>DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING</b>	<b>11</b>
<b>BCP</b>	<b>13</b>
<b>Data Retention Responsibilities</b>	<b>15</b>
<b>The Future of DRP and BCP</b>	<b>15</b>
<b>COMPUTER INCIDENT RESPONSE AND FORENSICS</b>	<b>16</b>
<b>Forensics</b>	<b>17</b>
<b>The Future of Incident Response and Forensics</b>	<b>18</b>
<b>PREDICTIONS</b>	<b>19</b>
<b>CONCLUSION</b>	<b>20</b>
<b>BIBLIOGRAPHY</b>	<b>21</b>

# The Future of Information Assurance

## *Techniques to Build Trust by Managing Risks*

“**M**ay you live in interesting times” is a well-known Chinese curse. Information Assurance (IA) practitioners and C-level business leaders are definitely living in interesting times. There is tremendous pressure on businesses to drive down costs, improve efficiency, and provide convenient connectivity and payment methods for customers. The only way businesses can meet these demands is to store sensitive customer, employee, and business data, and to make that data available to computing devices connected to public and private computer networks. The paradox is the systems that are supposed to lower costs and improve efficiency have created new costs to protect sensitive data from criminals both inside and outside the business.

Even if there somehow were a way that data were suddenly protected from theft or harm, the IA practitioner would still have much to do. They would have to insure the business systems remain available, that there is a continuity and recovery plan in place and tested in case of disaster, and they would have to make sure that the company’s employees know their roles and responsibilities regarding the company’s computing assets. The remainder of this report will look at these topics in more detail, and will attempt to predict how IA might evolve.

---

## Trust

Trust is the cornerstone of commerce, but trust is a very fragile thing. Trust is why IA is so important to businesses, whether today’s business leaders realize it or not. More and more business is being conducted online and businesses, health care providers, and social networks are storing more and more personal information on their networks. Cloud computing, which is the sharing of computing resources that are managed by a provider, is expected to make managing IT easier and more cost effective. These trends raise serious questions about security.

“Almost daily there are reports of massive exposures of personally identifiable information (PII), identity theft, distributed denial of service (DDoS) attacks, theft of thousands or millions of credit card numbers, botnets, malware, and other security breaches in electronic systems” (True “The Future of Information Assurance: A Prediction by a MSIA Student.” 3). Yet businesses continue to put themselves and their customers at risk by collecting, transmitting and storing sensitive information in an open format rather than encrypting it. They purchase or create software that is vulnerable to well-known exploits such as SQL

injections or Cross Site Scripting (XSS). They neglect to patch computer operating systems and software applications. They allow their data to leave the company through employee email or portable storage devices. They do not adequately isolate systems storing or processing sensitive data, putting these data at risk. One might logically conclude that the general state of IA is not very effective.

Why would a business, any business, operate with this much risk? There is no single answer, but possible answers include not understanding the problem, or a willingness to accept the risks, or some combination of both. Regardless of why business leaders have decided to operate with this level of risk exposure, they need to begin to think about the consequences:

- According to one security firm in the UK, “Almost half of Brits claim they wouldn't purchase goods or services from a company that had suffered a security breach.”
- “Research by CoreBrand assessing the impact of a negative incident on brand equity and shareholder value suggests that upwards of 10 percent of shareholder value can be tied to brand.”

Based on these statements, a company can establish a real competitive advantage if they are perceived as more secure and trustworthy than their competitors. Conversely, a business may lose considerable market share and shareholder value if they choose not to reduce their risk exposure.

## The Heartland Payment Systems Breach

“The CEO of Heartland Payment Systems, the company that suffered a data breach that exposed up to 100 million credit and debit cards, recently said in an interview, “...we certainly didn't understand the limitations of PCI and the entire assessment process. PCI compliance doesn't mean secure. We and others were declared PCI compliant shortly before the intrusions.”

Mr. Carr, the CEO of one of the biggest credit card processing companies in the world, did not understand the assessment process and that attaining PCI compliance does not mean that they were secure. Instead of taking responsibility for knowing his business and managing its risks, he blames the auditors. Such statements cannot inspire his customer's trust in his company” (True “The Future of Information Assurance: A Prediction by a MSIA Student.” 4).

Details of this breach are just coming out, mostly from the indictment of the defendants in the case. Here is security researcher, Rich Mogull's analysis of the breach based on what is known today:

- The attacks on Hannaford, Heartland, 7-Eleven, and the other 2 retailers used SQL injection as the primary vector.
- In at least some cases, it was not SQL injection of the transaction network, but another system used to get to the transaction network.

- In at least some cases custom malware was installed, which indicates either command execution via the SQL injection, or XSS via SQL injection to attack internal workstations. We do not yet know the details.
- The custom malware did not trigger antivirus, deleted log files, sniffed the internal network for card numbers, scanned the internal network for stored data, and exfiltrated the data.

Somehow the people responsible for IA at one of the largest credit card processing companies in the world failed to protect their systems from a well-known and understood attack, and if Mr. Carr is to be believed, they failed to adequately educate him about the difference between compliance and security.

What steps could and should Heartland have taken to secure their business and customer data?

- Perform vulnerability assessments
- Perform intrusion detection
- Perform egress filtering
- Create policies and an awareness program

## Vulnerability Assessment and Intrusion Detection

Vulnerability assessment systems (VAS) are capable of automatically scanning for and reporting on vulnerabilities in computer operating systems and software. VAS does not run continually, but can be automated to run on a pre-defined schedule. Some commercially available VAS are capable of detecting vulnerabilities in software such as SQL injections and XSS.

The current VAS capabilities are limited to known vulnerabilities. While some may view this as a severe limitation, the Heartland breach and several others are proof that the industry has a long way to go before it finishes addressing known vulnerabilities.

Intrusion Detection Systems (IDS) use known signatures to detect intrusions, and algorithms to detect abnormal traffic. Unlike VAS, the IDS runs continually and it alerts on violations. IDS can also be used to verify the quality and effectiveness of the firewall rules. Too often an administrator believes they configured a firewall rule correctly only to find out the hard way that they made a mistake. With an IDS in place, it can be used to alert on those types of errors and minimize the time the system is exposed.

Analogous to IDS is egress filtering. Many network administrators are very careful about the traffic sources into their networks but not about the traffic destination of traffic leaving their network. This is one reason malware and botnets are so successful, as they were in the Heartland breach.

Here is a brief summary of the benefits of VAS and IDS (True “Vulnerability Assessment and Intrusion Detection” 4):

- Periodic vulnerability assessments are required for PCI compliance (requirement 11.2)
- VAS and IDS help meet auditing requirements
- VAS reports vulnerabilities, and remediation reduces risk
- VAS can be used as a pre-deployment QA check
- IDS alerts in real-time when it detects a violation
- IDS helps with forensic evidence in the case of a computer crime (Kabay 2)

As we are beginning to see from the Heartland breach, there were steps that Heartland could have and probably should have taken that would have made it more difficult for the criminals to steal millions of credit card numbers. If they had properly installed, configured and managed VAS, IDS and software testing systems, they might have been alerted to the criminals’ activity before they could do damage. For example, if they had installed IDS and egress filtering between the sensitive cardholder subnetwork and the less secure, less sensitive subnetwork, they might have noticed the unauthorized activity.

## Software Vulnerability Assessment

Another form of vulnerability assessment that is useful is web application testing as outlined in the Open Web Application Security Project (OWASP) testing framework. Today’s computer criminals are bypassing the network and attacking businesses through the application layer; this is the vector the Heartland attackers used.

The OWASP testing framework suggests incorporating testing throughout the software development lifecycle (SDLC), including penetration testing to be conducted during the deployment phase.

## The Future of VAS and IDS

VAS, IDS, software and penetration testing are important forms of quality assurance, and are not likely to go away any time soon. In fact, their importance will increase as will the number of companies incorporating them into their networks. It is impossible to prevent every intrusion, so future systems will have to be able to dynamically respond to breaches. For example, the IDS could detect an intrusion and update the firewall rules to isolate the offending traffic.

Software development and testing will have to mature if the industry is going to meet its security challenges. Colleges and universities will have to teach secure programming, companies will have to train their developers and programmers how to write secure code, and security companies will create products to meet the demand for software VAS and

penetration testing tools. Customers will want some indication that the websites they visit are free from common vulnerabilities such as XSS and click jacking.

It will be extremely difficult for companies to claim ignorance once the lessons of this breach are shared with the industry. Future CEOs who attempt use the same excuses as Mr. Carr are in danger of finding themselves in court on charges of negligence. Regardless of any criminal or civil action that may or may not take place, they will certainly lose customer trust, market share and revenue.

## Security Policies and Laws

Security policies lay the foundation for any security program. ISO 27002 has the following objectives related to security policies (Praxiom Research):

1. Establish a comprehensive information security policy.
2. Make sure that your information security policy provides clear direction for your information security program.
3. Make sure that your information security policy shows that your management is committed to information security.
4. Make sure that your management supports your organization's information security policy.
5. Make sure that your information security policy shows that your management is prepared to support an ongoing commitment to information security.
6. Make sure that your information security policy is consistent with your business objectives.
7. Make sure that your information security policy meets your organization's business requirements.
8. Make sure that your information security policy complies with all relevant laws and regulations.

If a company's security policies meet these objectives, the thought is that they line-up with the business, the management and the laws and regulations to which the business is subject.

Having policies is good, but policies are worthless if only a few people are aware of them. Therefore, an awareness program is just as important as writing the policies themselves. Bruce Schneier suggests this method for creating awareness: "The risks of not following security procedures are much less real. Maybe the employee will get caught, but probably not. And even if he does get caught, the penalties aren't serious. Given this accurate risk analysis, any rational employee will regularly circumvent security to get his or her job done. That's what the company rewards, and that's what the company actually wants. "Fire someone who breaks security procedure, quickly and publicly," I suggested to the presenter. "That'll increase security awareness faster than any of your posters or lectures or newsletters." If the risks are real, people will get it."

The number of laws and regulations governing business has grown significantly in the past decade. The chart below lists some important laws and regulations related to IA (Cobb 6). In addition to these laws, 43 states plus the District of Columbia have data breach laws. These laws and regulations were written in response to acts of fraud and epidemic of data breaches.

RECENT LEGISLATION	WHO IS AFFECTED?	WHAT DO THE SECURITY PROVISIONS COVER?	WHAT ARE PENALTIES?	WHEN IS IT IN EFFECT?
Sarbanes-Oxley Act of 2002	All public companies subject to US security laws	Internal controls and financial disclosures	Criminal and civil penalties	Current law
Gramm-Leach-Bliley Act of 1999	Financial institutions	Security of customer records	Criminal and civil penalties	Current law
Health Insurance Privacy and Accountability Act (HIPAA)	Health plans, health care clearinghouses, and health care providers	Personal health information in electronic form	Civil fines and criminal penalties	Final security rule takes effect in April 2005
California Database Security Breach Information Act (SB 1386)	State agencies, persons, and businesses that conduct business in the State of California	Reporting of breaches of unencrypted personal information	Civil fines and private right of action	Current law
Federal Information Security Management Act	Federal agencies	Federal information, information systems, and security programs	Loss of IT funding	Current law
<b>Bottom Line</b>	<b>Significant impact on US private sector and governments</b>	<b>Financial, customer, health, personal and government information</b>	<b>Criminal and civil penalties and private right of action</b>	<b>Most provisions are already in effect</b>

## Censorship and Privacy in the Workplace

Many companies have policies that define what are proper uses of company computing assets and electronic communications. The purpose of such policies is to protect the company's data, reputation, and to avoid a hostile workplace. Companies monitor electronic communication in an attempt to enforce these policies. Awareness is the key to effectiveness of these policies just as with the security policies.

The Berkman Center for Internet and Society at the Harvard Law School cautions, "...policies regarding proper use of technology in the workplace, and the means that will be used to monitor such use, are highly recommended. Experts recommend that the notice be as specific as possible by including what types of monitoring will be used, how frequently monitoring will occur, and what purpose the employer hopes to accomplish through the monitoring. With an express privacy policy, an employee's expectation of privacy is avoided at least as courts have currently interpreted the law. Employment lawyers suggest that the policy be disseminated to all employees and agreed to by them, as well."

## The Future of Security Policies and Laws

A recent example of new laws is the American Recovery and Reinvestment Act of 2009, which establishes nearly \$1.2 billion in grants to help hospitals with the transition to electronic health records. As part of this act, Congress passed two laws to help insure security. SC Magazine's online version reported, "An interim final rule, issued Wednesday by the U.S. Department of Health and Human Services (HHS), requires health care organizations subject to *Health Insurance Portability and Accountability Act (HIPAA)* regulations to notify individuals whose information has been breached, when the breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals must be reported to the HHS annually.

The rule also applies to business associates of health care organizations.

"This new federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care," Robinsue Frohboese, acting director and principal deputy director of the HHS Office for Civil Rights, said in a statement. "These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information."

A similar final rule issued by the Federal Trade Commission this week requires web-based businesses that collect consumers' health information, including vendors and online applications that interact with PHRs, to issue notifications if a breach occurs."

Notice that the intent of the HHS rule is to maintain "consumer trust" as medical records are converted from paper to electronic format.

Considering the consequences for violating laws and regulations, policies will probably carry more weight than they do today, but awareness programs will probably be more sophisticated than simply firing people who violate policies. The penalty for violating security policies will have to be real when trust becomes a competitive advantage.

## Risk Analysis and Risk Management

Up to this point, this report has focused on building customer trust by assuring the systems are designed, configured and programmed securely. Companies are also judged on how they handle disasters and other service interruptions. Customers are getting comfortable interacting with companies at their convenience and are expecting them to be available. Frankly, businesses do not want to give their customers an excuse to check out the competition. This is where risk analysis and risk management come into play.

Risk analysis is difficult to do well because it is highly subjective. The method that is probably most common today is the Annualized Loss Expectancy (ALE) method. ALE attempts to estimate the cost of an event, how often it is likely to occur and compute the annual cost. For example, if an event is expected to cost \$1 million and is expected to occur once every 10 years, the ALE is \$100,000. The thought being that a company should not spend more than \$100,000 per year to mitigate this type of event. There are several problems with this method, mainly because there is not enough data available to make an accurate estimate of frequency of occurrence.

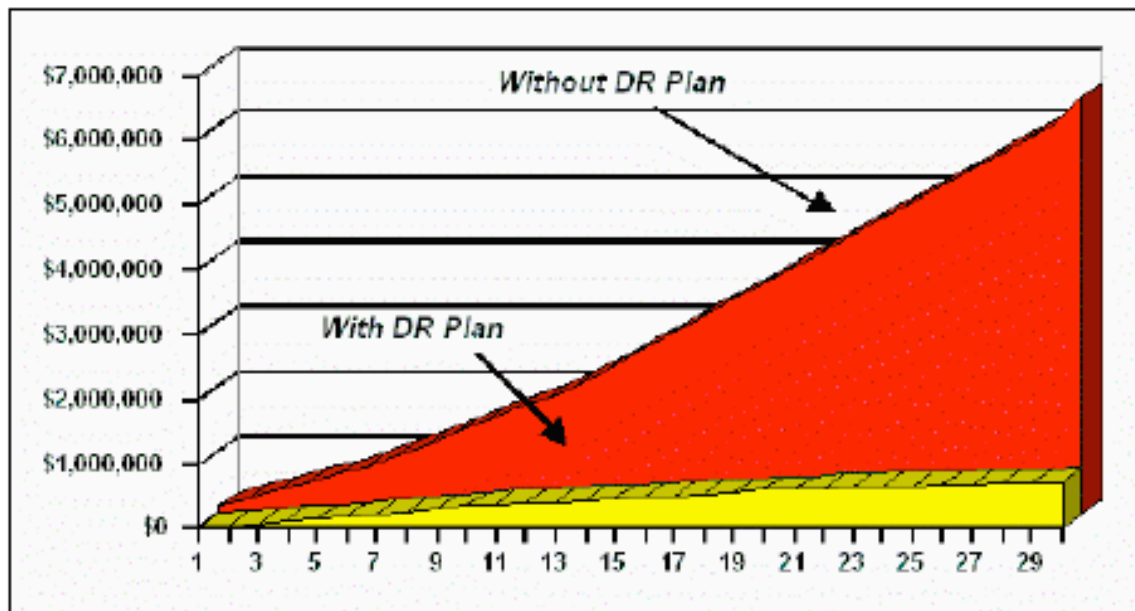
A better method is needed. There are at least three other possible methods from which to choose:

- The Gartner Group model focuses on the human threat: mean, motive, opportunity
- Formal Analysis of Risk in Enterprise Systems (FARES) focuses on threats
- Moira Generalized Cost Containment (GCC) model focuses on the cost impact of an event

Each of these models has advantages and disadvantages:

- The Gartner Group model is easy to explain and produces an actionable threat matrix, but is highly subjective and does not address environmental threats such as fire, accidents, power loss, and similar threats.
- FARES is capable of being fairly accurate over time, it is comprehensive and assumptions can be tested using simulated, but it is fairly complicated and expensive to model.
- GCC is easy to model and explain, and it is easy to build and costs very little, but it still relies on subjective data.

The GCC model may be the best method for most businesses. The GCC creates a cost estimate for each outage type as a function of time. The cost is applied only when the maximum downtime for that type is exceeded. First, the data is graphed as loss over time assuming no recovery plan. This is the red section in the graph below. Another dataset can be added to that graph showing loss over time with a recovery plan in place (yellow section) (Miora “Using the Generalized Cost Containment”). It is easy to demonstrate if the recovery plan meets ROI or not, which may be the most important outcome of the analysis.



## The Future of Risk Analysis and Risk Management

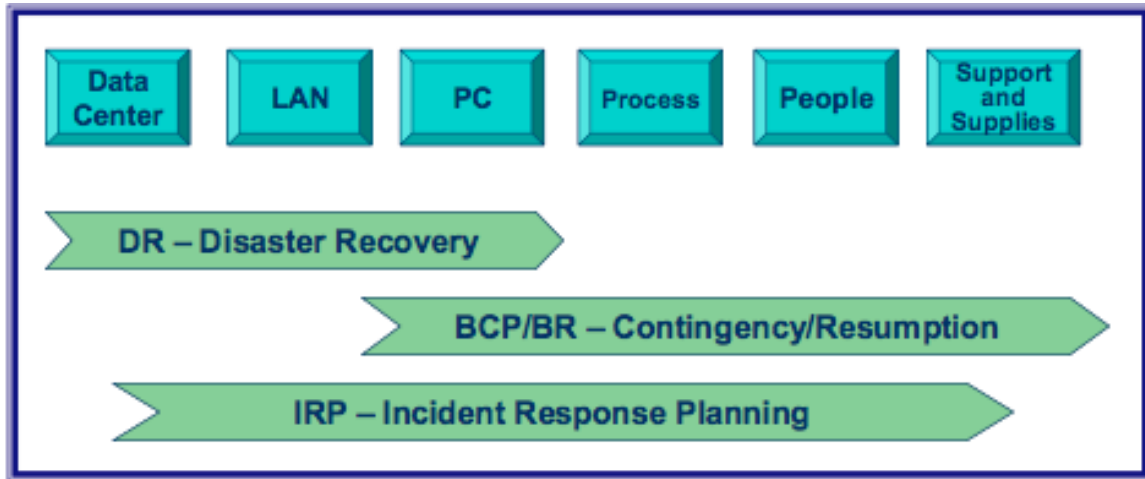
Risk analysis and management are critical components of any IA program. Both strategic and tactical decisions are based on the results of the risk analysis, and it can be extremely difficult to gain funding without demonstrating ROI. Unfortunately, there is no easy, low cost way to accurately develop this analysis at this time. Given the critical importance of this function, a better method will be developed, if for no other reason than more data will be available.

The responsibility for risk analysis will probably sit with a centralized authority in large organizations, and will probably be outsourced in smaller organizations. The reasons for this prediction are that risk management is a strategic function and it requires specialized skill and experience to do well.

## Disaster Recovery and Business Continuity Planning

The risk analysis should produce a list of threats and their potential costs. IA practitioners will prioritize these threats and create a plan to mitigate and recover from them. At this point in the process the focus is on the consequences not the cause. For example, it does not make much difference to the plan if a resource is lost due to a flood or to a fire, it is still lost and the recovery plan is the same. Many of these threats can be expected to result in the loss of hardware, data and possibly entire facilities and people. The diagram below shows how DR,

BC and Incident Response Planning relate to each other and to information resources (Miora “Incident Management and Response” 1).



The DR focus is on recovering from the incident or disaster, and a disaster does not have to be a malicious act on the part of man or Mother Nature. “No longer do we look at incidents as earthquakes or tornados, hackers or corporate espionage, terrorism or sabotage. Today, an incident can be any one or more of these, or can be something as simple as an accounting error that requires rebuilding and reestablishing financial baselines. It can be something as important as a breach of privacy that reveals private information about corporate customers. Any incident can cause corporate harm; every incident is less harmful if you see it coming” (Miora “Incident Management and Response” 2).

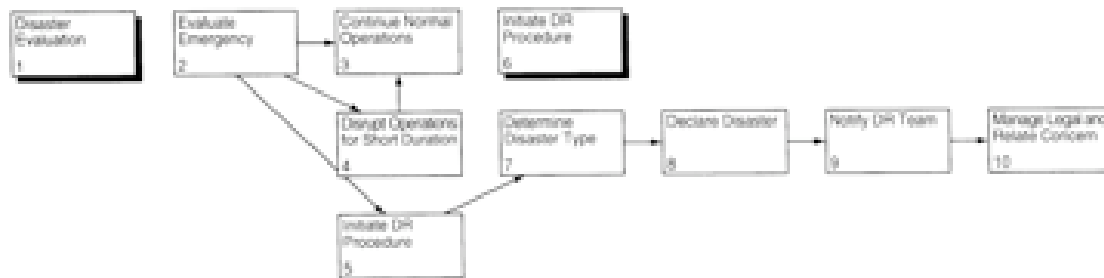
As illustrated in the above diagram, DR concentrates on restoring the data center, LAN, PCs and other infrastructure. These systems can be restored either by direct replacement or by using hot, warm, or cold sites. The decision as to which strategy to use is dependent on how long the business can afford to be down versus the cost of the recovery strategy.

Questions that might need to be answered as part of DRP include:

- How long can the business tolerate the loss of the affected information systems
- Which recovery strategy provides the best cost / performance ratio for our business
- How much computing power do we need
- How much storage capacity do we need
- How much power do we need
- How much air conditioning capacity do we need
- How much bandwidth do we need
- Which customers are affected by this incident and how will we notify them
- What communications resources will we need
- Is our network documented and where are the files stored

The answers to these questions are necessary to produce the DRP. The DRP will consist of

specific actions that the DR team will follow in response to an incident. The diagram below is an example of what a detailed DRP might look like (Miora “Chapter 43” 15). The first step is to evaluate the situation and decide if the situation should be declared a disaster, continue normal operations or to disrupt normal operations for a short time. If it is declared a disaster, the recovery team determines what type of disaster it is, declares it a disaster and notifies the DR team. The final step in this diagram is to “manage legal and related concerns.” Incidents need to be documented for several reasons including legal and insurance requirements, and for post event analysis purposes.



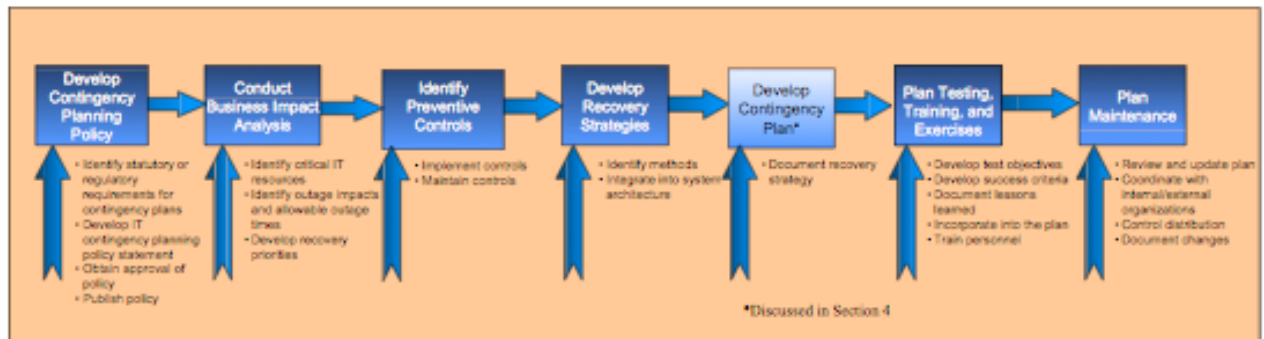
Once the disaster is declared, and the DR team activated, the team follows the detailed plan for that type of incident. The specifics depend on the answers to our earlier questions. Eventually the facilities and hardware infrastructure will be restored, and the continuity plan can begin. A final restoration, rebuild, relocation phase may be required, depending on the severity of the incident.

## BCP

BCP is about planning for restoring business operations after an incident. The location of operations may or may not be in the normal location, depending on the severity of the incident.

BCP development is one of seven steps recommended in the NIST publication, *Contingency Planning Guide for Information Technology Systems* (14):

1. Develop the contingency planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Develop recovery strategies
5. Develop an IT contingency plan
6. Plan testing, training, and exercises
7. Plan maintenance



Part of step 3, Identify Preventative Controls, is to identify recovery strategies. Recovery strategies can overlap with the DRP, especially where hardware and facilities are concerned. However, typically BC recovery strategies center on backup files and backup methods. Other strategies include load balancing and mirroring of servers and databases, especially in high availability environments. NIST suggests, “The selected recovery strategy should address the potential impacts identified in the BIA and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents” (19).

Policies should define how often backups should be created, where they should be stored, how they should be encrypted, and how they should be transported. Backups should be stored offsite; far enough from the primary site so as not to suffer from the same disaster as could affect the primary site. Options for storing backup files offsite include:

- Network Access Storage (NAS)
- Commercial storage providers
- Tapes, removable hard drives, DVDs or other portable media
- Cloud computing providers

It is extremely important to remember that these backups contain critical data including PII and should be protected. There have been too many instances where backup media is lost or stolen, unnecessarily exposing the enterprise to risks.

Step 4 is the development of the Contingency Plan. The goal is that the plan be clear enough that frontline employees can follow it. For example, people in the Systems Operation Center (SOC) should be able to pick up the plan and follow it until an incident commander relieves them. The NIST plan consists of 5 components (31):

1. Supporting information: project charter documentation
2. Notifications / Activation Phase: documents to define notification procedures
3. Recovery Phase: recovery priority, a recovery timeline, and recovery procedures; preferably including step-by-step checklists.
4. Reconstitution Phase: operations are returned to normal in the reconstitution phase.

5. Plan Appendices: vendor contact information including support contracts, hardware and network documentation, BIA, and other related documents.

## Data Retention Responsibilities

Related responsibilities in this area include data retention requirements as dictated by law. The organization must have a data retention policy and they must adhere to that policy or face fines and penalties. This is specific to eDiscovery laws. Other laws may apply depending on which industry the business is in. Here are some common examples (Herold 2,3):

### **Sarbanes-Oxley Act of 2002:**

- Fines and imprisonment of up to 20 years are proscribed for any person who corruptly alters, destroys, or conceals any records or documents to impair the use of them in any investigation.
- Failure to maintain audit/review work papers for at least 5 years can result in fines or imprisonment for up to 5 years.
- All audit and review information must be retained in a readily accessible and indelible format for 7 years.

### **Health Insurance Portability and Accountability Act (HIPAA):**

- Covered entities (CEs) must not only ensure the security and appropriate access to health information while in transit through networks but also while the information is in storage.
- Such information must be maintained for 6 years from the date of its creation or 6 years from the date for which it was last in effect, whichever is later.
- Penalties include not only civil, but also potentially large fines and/or prison time.

### **Gramm–Leach–Bliley Act (GLBA):**

- Financial organizations with customers and consumers who are United States citizens must implement security programs governing the security and retention of non-public personal information (NPPPI).

## The Future of DRP and BCP

Cloud computing will play a big role in DR and BC, because it is going to play a major role in normal IT operations. Businesses just want IT to work, and they want to focus on their core business, and cloud computing offers them that opportunity. It is a very flexible way for organizations to add or remove capacity as needed and not have to spend capital to buy the equipment nor do they need to pay staff to operate it.

Here is what one IT professional has to say on the subject, “So now commercial IT is loaded to the gills with stuff designed originally at an entirely different time when there were entirely different issues of scarcity, and that will change.

Because of the advancements of technology, CPU power, capacity, bandwidth (the things that our entire \$100B+ annual spend is based on) - all things once scarce - are now abundant

in IT. ... I HATE being in the IT business (and yes, I see the irony). We run VMware. We run Backup (CommVault). We run iSCSI and NAS (Dell and NetApp). We run HP dual-socket Quad-core Intel Xeon processors. We do all the same stuff everyone else does - just on a smaller scale.

I have zero desire, no offense, to have to pay people to keep this stuff working. It adds no value to my business. I am forced to be in the IT business. I would much rather spend the money focusing on adding value versus sucking value. I will be 100% in the cloud - as soon as it's realistic for me to be. I will focus on the real scarcity issues of TIME and MONEY. I will let others run infrastructure, as it is not core to my existence. I will focus on Op-Ex, and ultimately eliminate the Cap-Ex considerations altogether" (Duplessie).

Mr. Duplessie wants to let someone else run the IT infrastructure and he wants to lease capacity from them as he needs it. He believes that will free up his people to deliver better value to his organization. The responsibility for DRP and BCP at least as it pertains to data centers and servers will be transferred to the provider, freeing up even more time for his staff to work on other things.

## Computer Incident Response and Forensics

Computer incidents will happen so it is very important to be able to respond and investigate them. The main goals of an incident response team are to reduce the financial impact of the incident and return the systems to their desired state as quickly as possible. It is always best to be able to have a defined plan to follow when faced with an emergency or crisis situation. It is even more important when your actions may have to be explained in court. Therefore, organizations must create policies to define the scope and authority of the incident response team and create a plan before a crisis hits.

The following are steps that could be taken to create a plan (as modeled from the *Generic Computer Incident Response Team Plan*):

- Map threats to vulnerabilities
- Define skills / training / certification required for CIRT members
- Identify employees who have skills / training / certification required
- Define equipment required for monitoring / sniffing
- Monitor assets
- Define logging levels
- Define alarm thresholds
- Define response levels for each incident type (for example, Red, Yellow, Blue)
- Define team members for each response level at both the local and corporate offices
- Define incidents that will be escalated to law enforcement and the process for escalation to law enforcement
- Document contact information for all team members
- Document contact information for
  - ISPs

- Vendors
- Local and Federal law enforcement organizations
- Create a communications plan
  - Internal documentation
  - Internal communication
  - Public communication
- Create response plan for each alarm / incident type
- Communicate the plan to the organization
- Practice the plan

Different people will be required to respond based on the type of incident. This should be spelled out in the response plan. Each person should know what role they are expected to perform in response to each incident type as defined by the incident response plan. Types of skills/functions needed on a CIRT include (True “Computer Incident Response Teams” 4):

- System administrators
- Network administrators
- Security administrators and specialists
- Management
- Public relations
- Legal

This team has a good mix of skills needed to respond to an incident. The technical people can find and fix the problem, the PR people can communicate with the press and public, the management team has the authority to act and can communicate internally, and the legal people can insure any laws and regulations are met.

## Forensics

Computer forensics and incident response overlap to a certain degree. At some point in the incident response it may become necessary to collect or seize evidence. Consequently, it would be a good idea to treat every incident as if it will end up in court.

Computer forensics is a highly specialized skill and the results of the forensics investigation may be reviewed in a court of law. The people responsible for computer forensics must be highly trained and ideally possess industry and vendor certifications. Ideally, the organization would also have access to a lawyer who specializes in this field.

How the forensics investigation is handled has a direct impact on the ability to successfully prosecute the accused criminal. This reinforces the importance of creating a good response plan and practicing that plan so people know how to respond. The alternative is that people lose evidence or mishandle it, rendering it inadmissible in court.

The organization's security policies must detail who has authority to conduct a forensics investigation, the actions that a first responder must take, and when, how and who will escalate to law enforcement.

Information, especially computer forensics information, is extremely fragile, and it can be destroyed very easily if improperly handled. The Secret Service's *Best Practices for Seizing Electronic Evidence* document suggests these steps that should be taken by a first responder (p 2,3):

“Secure the Computer as Evidence

- If the computer is “OFF” do not turn “ON”.
- If computer is “ON”
  - Networked or business computers
    - Consult a Computer Specialist for further assistance
    - Pulling the plug could
      - Severely damage the system
      - Disrupt legitimate business”

Another critically important step is documenting what happened. This should be spelled out in the incident response plan, but it will be part of the evidence that is presented to law enforcement, or used in civil court.

Finally, eDiscovery is another category of computer forensics. Some companies have justified hiring computer forensics specialists due to the amount of eDiscovery work they must perform, usually in response to law suits.

## The Future of Incident Response and Forensics

Many businesses of all sizes do not have an incident response plan or forensics capabilities, nor do they have a provider lined up to respond. In the future, this will be unacceptable, as both businesses and the public better understand IA. Companies will probably be required to properly respond and investigate incidents, and escalate to law enforcement because their insurance companies and the laws are likely to require it.

Smaller organizations will probably need to outsource the incident response and forensics responsibilities to a managed security service provider (MSSP). Some larger companies may choose to outsource these functions if they decide they do not have the necessary skills, outsource their IT functions, or do not want to add staff.

The law is still being sorted out regarding computer forensics. For example, there is confusion over what evidence can be collected by a lay person and what must be collected or analyzed by an expert. As reported on the Federal Evidence Review blog, “Distinguishing lay and expert testimony can be a challenging feat, as other courts have recognized. *See, e.g., United States v. Hilario-Hilario*, 529 F.3d 65, 72 (1st Cir. 2008) (“There is no bright-line rule to separate lay opinion from expert witness testimony; circuits, and indeed decisions within a

circuit, are often in some tension.”) This same challenge can arise in considering computer forensic testimony. For example, can lay testimony be used to present results by “running commercially-available software, obtaining results, and reciting them”? The circuit noted that whether testimony about “computer-related” issues is expert testimony “is a relatively new question.” The Sixth Circuit addressed this issue and answered the question in the negative.”

The article concludes with the Court’s explanation, “The Sixth Circuit disagreed concluding that interpreting the results of the software tests required the witness “to apply knowledge and familiarity with computers and the particular forensic software well beyond that of the average layperson. This constitutes ‘scientific, technical, or other specialized knowledge’ within the scope of Rule 702.”

Imagine trying to account for such possibilities during a crisis.

## Predictions

- Companies will recognize the value of customer trust, and will manage their risks to maximize customer trust.
- The public will demand more secure information systems. This will be reflected in new laws and regulations, and new insurance rules.
- The cost and inconvenience of replacing debit and credit cards, or the nightmare of dealing with identity theft will cause the public to lose faith and trust in electronic payment methods.
- The cost and bad publicity of data breaches will cause businesses to focus more on IA.
- Security will become a competitive advantage, especially as some companies begin to differentiate themselves from their competitors in a way that the public understands.
- Many of these tactics require highly specialized skills. Consequently, many of these functions will be outsourced or centralized by larger businesses when it makes financial sense to do so.
- The market for MSSP will increase as more SMBs, and even larger companies require their services.
- Companies will decide that managing a MSSP is easier and cheaper than having a large security staff.
- Companies will use cloud computing and other service providers in an attempt to transfer risk.
- Cloud computing will be a factor in BC and DR, but there will be security incidents while the technology matures.
- Defense systems will get smarter and respond dynamically to threats.
- Software development and programming practices will include security testing throughout the SDLC.
- Software vulnerability testing will improve, and websites will signal to the user that they are safe from common vulnerabilities.
- The line between vulnerability assessment testing and penetration testing will blur.

## Conclusion

Wing Chun, a form of Kung Fu, has a saying, “When your opponent retreats, chase. When your opponent attacks, receive it.” What it means is not to fight against your opponent, but to use his energy against him. This system allows a physically weaker person defeat a physically stronger person. There are no planned or set responses to attacks, but it promotes the use of principles to neutralize attacks. The better one can apply these principals without thinking, the better they can neutralize and defeat their opponent.

Contrast this approach with how today’s computer security is applied. We erect firewalls, scan for vulnerabilities and patch holes. We attempt to detect intrusions, we establish long lists of rules for people to follow, and we try to account for every threat to our systems and build specific defenses against them. These are very static and programmed responses to threats, and leave these systems very vulnerable to new or blended attacks.

Our ability to deliver networked data and services currently outstrips our ability to deliver them securely. New methods must be developed, starting with the acceptance that threats exist and some will materialize. The information system must be able to respond to the threat, neutralize it and survive it. This is true whether the threat is man-made or environmental. After all, it does not matter to the business or to the customer why the system is not secure or unavailable, only that it is not operating the way that it should.

# Bibliography

---

## Works Cited

*Photo on cover page used with the gracious permission of Thom Gould.*

True, Becki. (2009). *The Future of Information Assurance: A Prediction by a MSIA Student.*

Skinner, Carrie-ann. "Brits Won't Use Firms Involved In Security Breaches". *Network World*. 8/15/2009 <<http://www.networkworld.com/news/2009/072809-brits-wont-use-firms-involved.html>>.

Johnson, Brian. "How Much is Your Customer's Trust Worth". *Free Online Library*. 8/15/2009 <<http://www.thefreelibrary.com/How+much+is+your+customer%27s+trust+worth%3F%28CONTACT+CENTER...-a0149302404>>.

Brenner, Bill. "Heartland CEO on Data Breach: QSAs Let Us Down". *CSO Online*. 8/15/2009 [file://localhost/http://www.csoonline.com/article:499527:Heartland\\_CEO\\_on\\_Data\\_Breach\\_QSAs\\_Let\\_Us\\_Down%3Fpage=1](file://localhost/http://www.csoonline.com/article:499527:Heartland_CEO_on_Data_Breach_QSAs_Let_Us_Down%3Fpage=1)>.

Mogull, Rich. "Heartland Hackers Caught: Answers and Questions". *Securosis*. 8/21/2009 <<http://securosis.com/blog/heartland-hackers-caught-answers-and-questions/>>.

"PCI Quick Reference Guide". *PCI Security Standards Council*. 6/13/09 <[https://www.pcisecuritystandards.org/pdfs/pci\\_ssc\\_quick\\_guide.pdf](https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf)>.

Kabay, M.E. (2005). *Managing VAS & IDS.*

True, Becki. (2009). *Vulnerability Assessment and Intrusion Detection.*

Cobb, Stephen. (2006). *Sox, SoDC, HIPAA & GLB: Recent Developments in Management Responsibilities & Liabilities for IA Practitioners.*

"ISO 27002 (17799) Information Security Control Objectives". Praxiom Research Group.  
8/5/09 <<http://www.praxiom.com/iso-17799-objectives.htm>>.

"Privacy in the Workplace". Berkman Center for Internet & Society. 8/1/2009  
<[http://cyber.law.harvard.edu/privacy/Module3\\_Intronew.html](http://cyber.law.harvard.edu/privacy/Module3_Intronew.html)>.

Moscaritolo, Angela. "Healthcare Breach Notification Mandated". SC Magazine.  
8/21/2009 <<http://www.scmagazineus.com/Health-care-breach-notification-mandated/article/146976/>>.

Miora, Michael. 2002. *Using the Generalized Cost Containment (GCC)*.

Miora, Michael. 2006. *Incident Management and Response*.

Miora, Michael. Chapter 43.

Swanson et al. 2002. *Contingency Planning Guide for Information Technology Systems*.

Herold, Rebecca. *Data Retention Compliance*.

Duplessi, Steve. "Steve's IT Rants". 8/22/2009  
<[http://esgblogs.typepad.com/steves\\_it\\_rants/2009/08/scarcity-imbbalances-why-the-smb-and-the-cloud-will-change-the-game-.html](http://esgblogs.typepad.com/steves_it_rants/2009/08/scarcity-imbbalances-why-the-smb-and-the-cloud-will-change-the-game-.html)>.

Brussin, David and Stephen Cobb and Michael Miora. 2003. *Generic Computer Incident Response Team Plan*.

True, Becki. (2009). *Computer Incident Response Teams*.

US Secret Service. 2002. *Best Practices for Seizing Electronic Evidence*.

Editor. "Drawing The Line On Computer Forensic Expert And Lay Testimony (Part I)".  
*Federal Evidence Review*. 8/22/2009  
<<http://federalevidence.com/blog/2008/october/drawing-line-computer-forensic-expert-and-lay-testimony>>.