

Global exploitation scanning and system infiltration is a non-stop daily assault by highly skilled criminal organizations.



**Are you prepared to respond?**



For more information please email [processone@acmbs.com](mailto:processone@acmbs.com) and a representative will contact you.

**Corporate Headquarters**

ACM Business Solutions, LLC  
407 Wekiva Springs Rd, Suite 241  
Longwood, FL 32779

**Regional Locations**

Charlotte, North Carolina  
Jacksonville, Florida  
Tampa, Florida

866-788-1505 Toll Free | 407-788-1505 Phone | 407-788-0316 Fax | <http://www.acmbs.com>

© 2010, ACM Business Solutions LLC, Process One™ and the Process One™ logo are registered trademarks of ACM Business Solutions LLC. All other registered trademarks and servicemarks are the property of their respective owners. All rights reserved.



## Protecting Your Business

A Process Driven Approach to Security Case Management

*“Our corporate security has been compromised. Vital intellectual property and sensitive data could have been stolen. The crucial steps we take could either neutralize the impact or become front page news. Which direction will our process take us?”*



*“Do we have the right processes and tools to minimize our exposure to costly litigation and downtime? Or even worse, possible **irreversible damage** to our reputation and image?”*

*“How will a security incident affect shareholder value, competitive market advantage, or an active acquisition? How will we protect customer, vendor and investor relations?”*

*“Who needs to be informed, how and when?”*

*“What are the policies and procedures, and do we have a system that will enforce them?”*

**Will you be asking these questions or will your team be actively responding?**

## Understanding the Risks

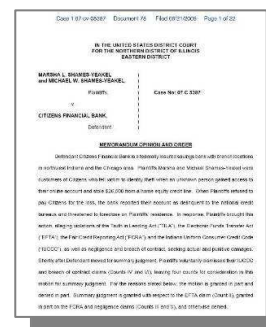
Computer Security Incidents have become severe and sophisticated. Risks range from disruption of business operations and lost or stolen laptops, to **coordinated theft of digital assets such as; payment card data, bank account access, and personal identifiable information used in Identify Theft rings**. Digital industrial espionage occurs frequently and range from external hacking to steal trade secrets, to soliciting **trusted insiders to “mine” intellectual property**. Compromised trade secrets may result in immeasurable costs to lost business opportunity and market position. Cyber Warfare is even being waged by both legitimate and rogue nations attempting to uncover and extract state secrets.

Industry studies have shown that in 2010 96% of the viruses detected function as a component of an underground, market-based mechanism termed "Crimeware-as-a-Service." **Crimeware automates collection and harvesting of valuable data** through large-scale attacks that generate multiple revenue streams for criminal enterprises. Crimeware will primarily target data for identity theft in order to access online banking services, shopping transactions, and other Internet services.

Based on recent estimates, Cybercrime has evolved into a **\$1 trillion a year global market**. Reports have found that in the U.S. alone the direct average cost to a large organization is **\$3.8 million per year just to respond, mitigate and clean-up** after security incidents. The average time required for an external breach is **fourteen days**, while insider attacks can take up to **forty-two days** or longer.

Even with the best cutting-edge technologies there are no guarantees that tools can completely safeguard against policy violations and malicious attacks. **How effectively organizations respond** to an incident is now more critical than ever.

**“Your system will be breached. This is not a question of “if” but “when”, and when it happens you need to demonstrate reasonable preparation for an event.”** ~ Theodore F. Claypoole, Co-Chair, Cyberspace Privacy and Data Security Subcommittee, American Bar Association's Business Law Section.



As new threats arise, legislation and industry regulations become more rigorous and **continually drive corporations to elevate** their security posture and awareness.

There can be **harsh legal liabilities**, including **compensatory and punitive damages** resulting from a single computer security incidents.

Unlike the theft of a physical object, theft of **digital assets can never be fully recovered** since there is a potential for unlimited distribution.

When a company falls victim to a security breach, especially if it involves exposure of customer data or intellectual properties, the **true cost to future business** is impossible to measure.

**Apple's Worst Security Breach: 114,000 iPad Owners Exposed**

Apple has suffered another embarrassment. A security breach has exposed iPad owners including dozens of CEOs, military officials, and top politicians. They—and every other buyer of the cellular-enabled tablet—could be vulnerable to spam marketing and malicious hacking.

The breach, which comes just weeks after an employee lost an iPhone prototype in a bar, exposed a list on the planet, a collection of early-adopter subscribers that includes thousands of A-listers in finance, politics and media, from New York Times Co. CEO Janet Robinson to Diane Sawyer of ABC News to film mogul Harvey Weinstein to Mayor Michael Bloomberg. It even appears that White House Chief of Staff Rahm Emanuel's information was compromised.

It doesn't stop there. According to the data we were given by the web security group that exploited vulnerabilities on the AT&T network, we believe 114,000

## Responding to Risks

In response to the escalating liabilities an organization will be faced with, computer security incident case management has also matured. Companies are forming a dedicated **Computer Security Incident Response Team (CSIRT)** comprised of subject matter experts in their respective fields.

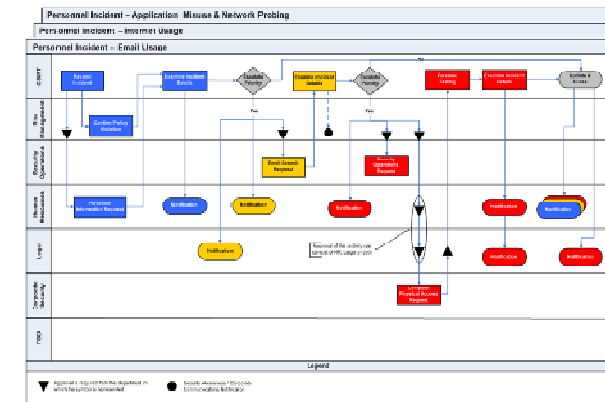
CSIRT is a cross-functional group that works closely with internal and external authorities to respond to an incident, and maintains secure records and artifacts of their analysis. In a Law Enforcement terms **CSIRT is the Crime Scene Investigators**.

Case types range from simple policy violations and targeted external attacks, to potential cases of internal industrial espionage. CSIRT and Security Incident Case Management is not simply digital forensics; it is a **business process and a strategy** to defend your organization and prevent future threats.

**“Back in my day, I would probe by hand. Now you can get commercial software that does the job for you.”** ~ Kevin Mitnick, Computer Security Consultant and Author (reformed hacker)

## Unifying CSIRT and Security Incident Case Management

At the core of an effective CSIRT Program is the detailed business analysis of **events or conditions that trigger an incident**, and the procedures that are followed to respond and bring an incident to closure.



The response activities and prioritization are based on a unified view of the business impact of each incident type. Specific tasks and approvals (work-flows) are unique to each incident based on the business rules. This set of policies and procedures are commonly referred to as the **“CSIRT Playbook”**.

Without this incident context, organizations can experience poor coordination, waste valuable time chasing “false positives”, overlook critical characteristics of greater threats, and will generally operate in an ad hoc and reactive mode.

A well planned CSIRT Program and Security Incident Case Management framework will **enforce a proactive, controlled and repeatable process**. This enables an organization to continually mature their security posture and preparedness.

ACM Business Solutions has leveraged decades of Security, Governance, Risk and Compliance experience to develop Process One™, an integrated Security Incident Case Management solution. **Process One™ unifies an organization’s CSIRT Program with a best-practice CSIRT Playbook**, provides real-time status on all computer security incidents with a complete audit trail.

Process One™ is a flexible business solution which easily adapts to the unique requirements of each client **without the need for code-level customization**. Process One™ fuses the CSIRT Program with an intuitive browser-based Security Incident Case Management solution enhancing the organization’s Risk Management strategy.