



Draft White Paper

---

## **Enhancing Cyber Security with Information Sharing Planning (ISP) & Playbooks**

---

David Kamien  
CEO, Mind-Alliance Systems, LLC  
November 2011

# Enhancing Cyber Security with Information Sharing Planning & Playbooks

In the typical enterprise, the effort to manage risk and strengthen resilience is fragmented across business units, disciplines, and organizations, and it is rare to find people, process, and technology that are truly well coordinated.

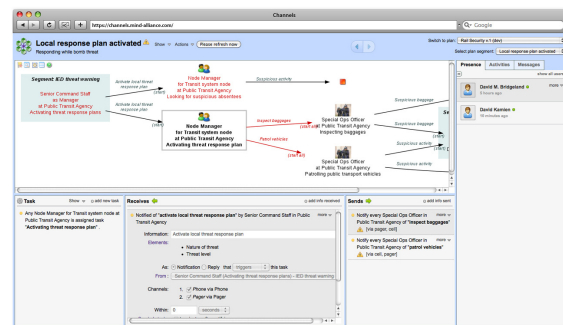
The effort to protect enterprises from cyber threats is no exception to this lack of coordination. In an effort to detect and identify anomalous behavior and eliminate threats – ideally before vulnerabilities are exploited and intellectual property and sensitive information are stolen -- an organization typically deploys many point solutions for security event correlation and application management, IT systems, and network infrastructures.

Responsibility for security is split between IT, accounting, legal, HR, and the security office itself, and each discipline has its own stakeholders, technical jargon, and regulatory compliance obligations (e.g., SOX, PCI, FISMA, HIPAA).

Chief Information Security Officers (CISO) need a new conceptual framework and management system for harmonizing the efforts of security stakeholders across the enterprise. This is key to strengthening coordination and unity of effort in risk management. Information Sharing Planning and the development of guidelines or “playbooks,” are essential in this context. Playbooks specify what to do and who to communicate with when security-relevant events<sup>1</sup> are identified, whether by an automated monitoring program or a human being. Playbooks should contain procedural workflows determining which standard actions each role (Level-1 or Level 2 analyst, incident responder,

engineer, operations manager, etc.) should be trained to take in reaction to each actual or potential cyber threat event. These playbooks might include interaction not only with people or systems internal to the organization, but also those in partner organizations, such as vendors.

Enterprises should build a comprehensive library of “playbooks” for all actionable cyber incidents and use them to train personnel to ensure that they know what tasks to recommend or execute, and what information about vulnerabilities, threats and response action to include in communications they send or request (e.g., threat reports, incident summaries, and investigation reports). Establishing a formal cyber security Information Sharing Planning process with the help of the Mind-Alliance Systems’ CHANNELS software allows you to formalize a framework for producing these playbooks.



**CHANNELS outputs procedures that can be appended to plans and training material and integrated into other applications.**

Effective information sharing with partners inside and outside the enterprise enhances understanding of new security threats and yields new insight into effective prevention, protection, and response action strategies. This is essential because criminals are continuously launching innovative and technically sophisticated attacks--blended threats that combine physical and cyber offensive action and exploit new vulnerabilities in your network

defenses.<sup>ii</sup> Information sharing can help to determine which, out of the thousands, that indicate a potential security threat to business critical IT assets, need to be prioritized/triaged and require a “critical” incident response. When an event is detected, and deemed actionable, it may result in callout and display of an alert in analyst active channels, via a dedicated team page, or on a situational awareness dashboard. Depending upon the level of alert, it may be included in a daily email report to the vulnerability team, triggering an investigation, ticket and case management, or additional monitoring. By sharing information effectively with internal stakeholders and partnering with external organizations, enterprises can extend the virtual security perimeter and detect threats sooner, reducing exposure and minimizing adverse impacts.

ISP provides a way to continually measure and improve the efficiency and effectiveness of the cyber incident reporting process. Sharing threat intelligence and the insights gained from network security, application testing, and security-monitoring efforts enables organizations to better manage risk by patching or preventing vulnerabilities. In this way, Channels is a valuable addition to any security, intelligence, or risk management system because it enables enterprises and their partners to achieve greater unity of effort, supports audits, and demonstrates compliance with critical regulations.

Information Sharing Planning procedurally integrates human intelligence (which cannot be automated) and technology-based automated cyber and physical security systems to deliver unified risk and security intelligence that helps:

- Gather and analyze network and system security data in real-time

- Achieve rapid situational awareness of current threats and compliance requirements
- Implement a monitoring program which accurately identifies, analyzes, and correlates security events and vulnerabilities with contextual data
- Escalate actionable events and alerts on compliance exceptions
- Expedite threat elimination and vulnerability remediation and accelerate incident response times
- Minimize the impact of adverse events that do occur
- Continually measure the effectiveness of security processes
- Automate the monitoring and enforcement of security controls and compliance processes
- Fully integrate people, process, and technology into the lifecycle of security events

---

To learn more about **Mind Alliance** visit [www.mind-alliance.com](http://www.mind-alliance.com) or call **1-888-731-6018**.

---

## **i Examples of Events**

- Shared account user attribution
- Botnet activity detected
- New virus outbreak
- Successful attack / malicious code
- SQL injection
- New vulnerability on DMZ host
- Suspicious activity / statistical anomaly
- New pattern of activity detected
- Unauthorized Root/Admin Access
- Unauthorized user access (explicit or by role)
- Successful Denial of Service
- Attempted unauthorized access
- Malware infection
- Policy violation
- Reconnaissance
- Phishing
- PCI data card path circumvented

## **Associated Systems**

- Databases
- Physical infrastructure
- Identity management
- Firewall/VPN
- Intrusion detection systems
- Network equipment
- Vulnerability assessment
- Anti-virus applications
- Directory services
- System health information
- Web traffic

---

## **ii Shadows in the Cloud**

A joint report from Information Warfare Monitor and the Shadowserver Foundation (available <http://www.nartv.org/mirror/shadows-in-the-cloud.pdf>) points to a disturbing complex ecosystem of malware networks, cyber crime and espionage. The report shows how these networks can be aggressively adaptive systems, multiplying and regenerating across multiple vectors and platforms, and exploiting the vulnerabilities within the latest Web 2.0 technologies to expand their reach and impact.