



**Reorganizing Intelligence**  
**infectionvectors.com**  
**March 2005**

## **Overview**

Recently, President Bush has made headlines with a plan to reorganize the United States' intelligence programs. This effort is intended to improve the communication and effectiveness of the various groups involved in national security, bringing together multiple agencies under a single command. In all types of organizations there is a need to share information and leverage the specific skills of diverse groups. Regardless of how one feels about the specific plans of President Bush, the idea is worth evaluating for every group when it comes to malware defense. This report identifies the major tenets of such reorganization, how it might work in practice at a large organization, and the benefits when applied to virus defense. The type of "reorganization" mentioned here is not nearly as sweeping a change as proposed for the US intelligence community, but rather a logical organization of the skills required to deal with malicious code efficiently.

## **The Status Quo**

Presumably, the reason to consider reorganization is that there is a perceived or demonstrable problem with the integrity of malware defense at an organization now. This may be the result of a virus outbreak, a fairly common occurrence within large companies. It may also be a result of examining the configuration management (CM) teams and process improvement practices within the company. Often, when analyzing the review teams and decision-making forces inside an organization it becomes apparent that the subject matter experts are not "in the loop" when it comes to malware defense. Reorganizing malware intelligence is a process that identifies where malicious code expertise lies in a company, who is best in a position to analyze/implement defensive modifications to the corporate network, and then how to ensure that these individuals collaborate during outbreaks that affect the enterprise.

## **Defragmenting the Team**

Malware intelligence is likely scattered around a large IT shop. The first thing to evaluate is where the interest and experience resides. This may require just walking around and talking to people, it is often surprising who is personally interested in the virus/anti-virus world. Although a number of security folks will likely answer up, there may well be a few others in the shop already. These people make great additions to a malware defense team. Their proximity to internal practices and breaking virus news sources puts them in a good position to help identify new threats and specifically those that pose a significant risk to the organization.

Others that make good virus defenders are those responsible for security policies: both in terms of crafting them (at every stage, don't leave out management) and enacting them (the technical people in the server rooms). The technical team needs a broad range of talents to match the varied forms of malicious code: email, Internet worm, file infector, file share worm, etc. These characteristics require skills with the mail relays/clients, patching process, file systems, network security configuration and rights. The skills are not directly related to understanding viruses and worms; there is a need for much more than just malware analysts. The table below shows the relationship between some malware traits and the respective support personnel that will be required to successfully and efficiently combat them:

TRAIT	NON-MALWARE SUPPORT KNOWLEDGE
Email Propagation	SMTP/Mail Relays
Network Vulnerability	TCP/IP; OS Security Alerts/Patching
File Infector	File system; OS
Web/Client-side Scripting Attacks	Web Services; Alerts/Patching
Web/Server/Application Injection	Application Security

During a security review of the organization, the list will be populated with the services and applications that actually exist within the enterprise and the respective skills required to support them. Proprietary applications require additional specialized (often in-house) expertise that shouldn't be overlooked.

Measuring the defensive posture of an organization is explored in other infectionvectors.com reports; please see:

[http://www.infectionvectors.com/emergprep/meas\\_success1.htm](http://www.infectionvectors.com/emergprep/meas_success1.htm)  
[http://www.infectionvectors.com/emergprep/meas\\_success2.htm](http://www.infectionvectors.com/emergprep/meas_success2.htm)

Or contact infectionvectors.com for additional information and organization-specific support.

### **How Does It Help?**

With the focus on business metrics, mechanisms by which processes are measured to validate success, it is reasonable to ask how such reorganization may help improve the security posture.

Much like the plan to reorganize the US intelligence community, the goal of a malware defense team is to centralize the malicious code expertise and streamline the response effort. This team will fit into existing CM procedures and into any integrated project team (IPT) that may exist for security issues. This approach is very much like collecting capabilities for any enterprise – when a need arises for action on a virus or worm threat (directed by information assurance folks, see the “Malcode Process Model” at

infectionvectors.com for an outline) the important players will be identified, briefed, and ready to provide recommendations on defense and remediation. Also as important, they will be ready to explain why certain steps may be too resource intensive to justify (where there is no “bang for the buck” so to speak). Finally, there will be enterprise-wide buy-in and knowledge dissemination, a key area missing from many large networks.

How is this measured? If existing metrics are in place to identify the time taken to mitigate external attack threats, including the patching process and time between alert and mitigation, then there is already an infrastructure for measuring these tactics. Return on investment metrics should also show an improvement with respect to cost of tools and defense strategies. Often experts in one area of technology (that is not traditionally considered a “security” tool) can use their tools to mitigate worm attacks. This is especially true with system administrators handy with scripting and systems management platforms.

### **Filling in the Holes**

The exercise of collecting malware and malware defense expertise may result in finding that the gaps are too great to overcome internally (because of costs, time, personnel constraints, etc.). After considering the skill set needed, the organization will likely find discrepancies between what they feel is necessary and what exists in-house. In all but very large enterprises, supplemental support for security services is probably required. This can be as simple as visiting security websites for information on the latest threats to hiring managed security providers to maintain one or more facets of the organization’s malware defense.

Even in cases where the enterprise is prepared to outsource malware defense, it is vital to have a response team organized to deal with emerging threats. In the smallest companies, this means collecting the on-call phone numbers of external systems support. In larger enterprises this will involve tapping the types of role players noted above. In all cases, organizing the response effort before a malicious code emergency will greatly improve the speed of mitigation actions.

