Methodology for Cyber Effects Prediction

W. Shane Powell, CISSP-ISSEP
Principal Systems Security Engineer
Raytheon, Network Centric Systems

Version: (1.0)
January 22nd, 2010

Table of Contents

Table of Figures

Now the general who wins a battle makes many calculations in his temple ere the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: how much more no calculation at all! It is by attention to this point that I can foresee who is likely to win or lose.

- Sun Tzu, the Art of War

1 BACKGROUND

Once the sole domain of military planners, public sector organizations must begin to understand the extent to which cyber attacks may affect their ability to conduct mission essential operations. Various information security regulations and standards aid organizations with configuring information systems securely. Common processes are used to assess system vulnerabilities and assign risk. However, vulnerability and risk assessments can easily mislead system owners into a false sense of security. While vulnerabilities can be patched and risks may be mitigated, the end result is inevitable that someone must accept responsibility should their organization fall prey to cyber attack through exposures that remain.

The Methodology for System for Cyber Effects Prediction as discussed in this paper makes use of traditional and emerging technologies, along with analytic methods to provide a deep understanding of the actual security state of an organization's information systems. Cyber Effects Prediction harnesses detailed knowledge of how an organization's information systems are configured, business operations are conducted, continuity of operations are planned, and external relationships are trusted. The Methodology for Cyber Effects Prediction can be used to collect and correlate information concerning how information systems will likely be attacked, allowing for prediction of the cascading effects that would result from successful cyber attacks.

Knowledge derived from Cyber Effects Prediction allows for:

- Understanding System Security Baseline Configurations
- Assigning System Criticality According to Organizational Mission
- Understanding Internal, External, or Hybrid Organizational Exposures to Cyber Attack
- Understanding the Reach of Cyber Attacks Vectors crossing Organizational Exposures
- Identifying Primary (Direct) Cyber Effects Affecting Systems
- Predicting Secondary (Internally Cascading) Cyber Effects Affecting Distributed Services
- Postulating Tertiary (Externally Cascading) Cyber Effects Affecting Operations and Mission
- Demonstrating System Vulnerabilities through Targeted Penetration Testing
- Identifying and Prioritizing Remediation Actions
- Allocating Resources Efficiently in Support of Remediation Actions
- Calculating Residual Risk either Qualitatively, or More Importantly, Quantitatively

The methodology described throughout this document, and illustrated in Figure 2-1, focuses on applying Cyber Effects Prediction to the defense of information systems.

2 METHODOLOGY

The Methodology for Cyber Effects Prediction consists of four major components.

1. System Security Baseline Configuration
2. Modeling, Simulation, and Analysis
3. Vulnerability Demonstration
4. Allocation of Remediation Actions and Residual Risk

Each component builds upon the products of the previous component. In their entirety, the methodology provides system security engineers with a framework against which they can establish the current security state of their system, make assumptions on the affect of exploits used against current or potential weaknesses in their system's security state, and to validate security configurations or weaknesses.

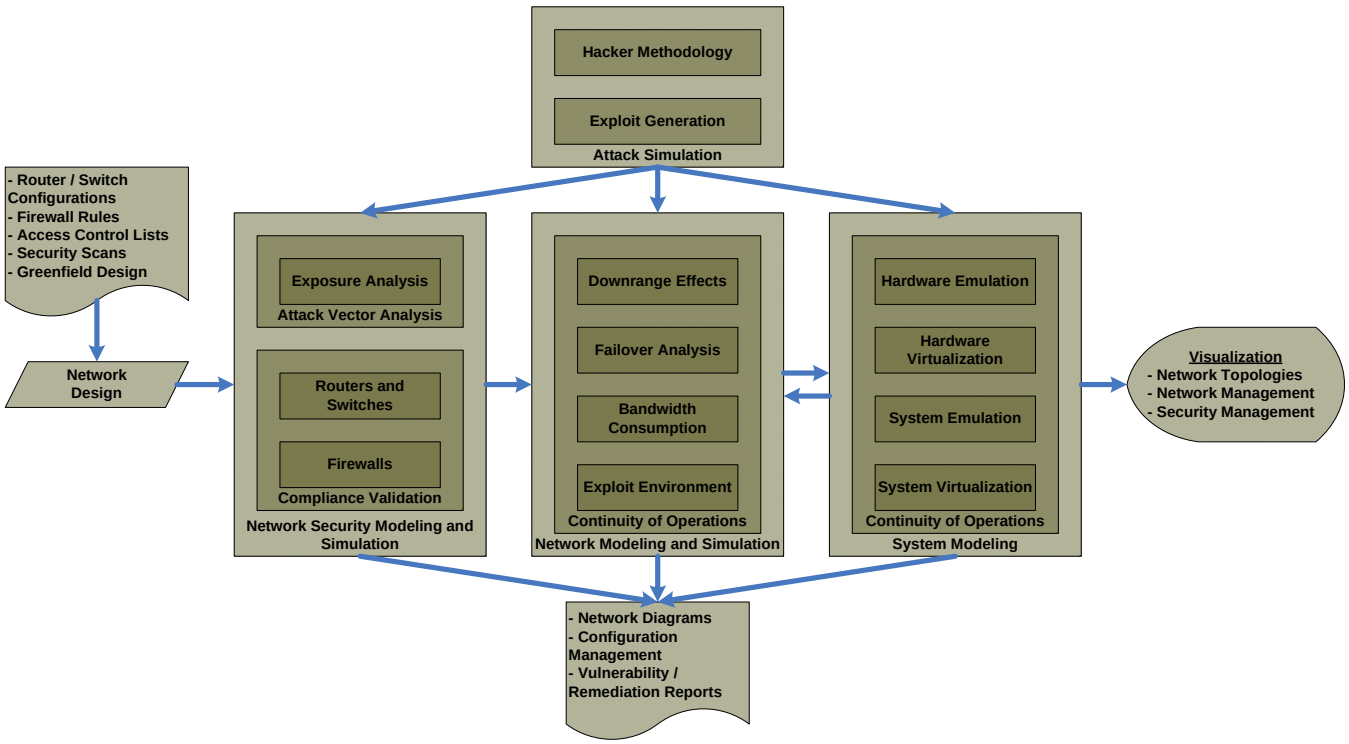

Figure 2-1 - Methodology for Cyber Effects Prediction

2.1 SYSTEM SECURITY BASELINE CONFIGURATION

Failure for a battlefield commander to understand the terrain that will be fought on during a land-based war results in defeat. The same principle holds true for the manager of a security operations center. If the cyber battlefield is not understood, it will inevitably fall to exploitation from persistent cyber threats. In either case, it is imperative that the battlefield commander or security manager understand the terrain of the battlefield that they must fight on.

In order to defend information systems from persistent cyber threats, it is absolutely necessary to possess a firm understanding of the system's overall security state. Not only does this require well

documented system configurations, network infrastructures, and vulnerability assessment scans, it requires that these discrete data sources be fused into a unified operational representation of an organization's cyber battlefield. It is within this cyber battlefield that an organization's electronic and information assets are defended.

A system's security baseline can provide a highly accurate representation of the system, which allows the execution of further analysis. Standard network mapping, vulnerability scanning, and network management tools, are used to collect system state data needed to build system security baselines.

System configurations and security state data collected during this stage of cyber effects prediction are correlated using security modeling, simulation and analysis tools. Vulnerability assessment tools, along with network configurations provide a snapshot of the system's security baseline at a given point in time. These snapshots can then be used for differential analysis to determine if changes that occur within the system over time degrade its overall security state. Ideally, pristine baseline configurations are available to systems security engineers. This is rarely the case, and effort is required to capture the most complete baseline feasible.

Using a current system security baseline, an analyst or engineer can perform the complex fusion analysis which needed to understand the system's overall security state. Not only does this allow for the analysis of organizational exposure and attack vectors, it facilitates the discovery non-obvious vulnerabilities and effects.

2.1.1 Host Scanning

2.1.1.1 Non-Authoritative Vulnerability Scans (Port Scans)

Basic vulnerability scans are conducted from within the same network segments as the systems assessed. Doing so ensures that switching or network security devices do not block or modify scan traffic as it is routed through network infrastructures. This class of vulnerability scans is considered non-authoritative because results are in essence estimated. Much of the system state data collected in this manner is published to networks by the systems being scanned in order to support interconnectivity. However, systems implementing the principle of security through obscurity will publish false data, if the systems scanned respond at all.

Additionally, some system state data is assumed based on common configurations, as is often the case with the detection of services through these types of scans. As a result, the vulnerabilities reported for the systems scanned may indeed be incomplete or even false. From a defensive perspective, non-authoritative vulnerability scans should be performed in conjunction with network mapping activities as a method of validating network topologies that are declared by system owners. This ensures that systems are not intentionally or unintentionally left out. While useful during network mapping, insufficient data is returned to facilitate the full capture of system configurations needed. Initial data points derived from non-authoritative vulnerability scans may include:

- IP Addresses and Host Names
- Open or Listening Ports
- Service Banners
- NetBIOS Information
- Domain Name Listings

- Public Shares

2.1.1.2 Authoritative Vulnerability Scans (Internal System Scans)

Authoritative, or credentialed vulnerability scans often begin with non-authoritative scans to assess what is visible to attackers. However, their reliability comes from authenticating to systems being scanned using administrative credentials. In doing so, this method of scanning has direct visibility into all of the files and configuration settings that an administrator has access to. Execution of scripts delivered to scanned systems allows for the collection of the precise data points necessary to establish highly reliable system security states.

While this approach can be limited if root-kits are present or credentials are used that do not possess sufficient privileges on the systems being examined, this represents the most accurate approach to capturing system configurations and security states. In addition to system state data that may be available to non-authoritative vulnerability scans, use of credentials allows the collection of data such as:

- Services and Associated Applications
- Build Levels for Operating Systems and Applications
- Network Device, Operating System, and Application Specific Configurations
- Domain Configurations
- User and Administrator Accounts
- Local and Domain Group Policies
- Hidden Shares

2.1.2 Network Switching and Security Devices

Often overlooked during security evaluations, network device configurations provide system state data needed to validate defense-in-depth issues relating to network infrastructures. Switching devices define how networks are segmented, or facilitate communications with other networks. Network security devices define how network sensors are deployed, and the specific security controls that are in place to limit the effects of cyber attack across network connections.

When assessed, these devices must also be evaluated for vulnerabilities using authoritative scanning techniques. The reason for this is simple. If the network device itself can be compromised and administrative access is gained, other routing and security mechanisms controlled by the device can be modified to support further cyber attack. Examples of data collected from network devices include:

- Router / Switch Configuration Files
- Load Balancing Configurations
- Access Control Lists
- Firewall Rules
- Intrusion Detection / Protection System Rules

2.2 MODELING, SIMULATION, AND ANALYSIS

Analysts can gather an enormous amount of information through vulnerability assessment scanning and the collection of network device configurations needed to support system security baselines. Consolidating the information gathered into a concise model can ease the effort needed to adequately assess network and system security. Once consolidated, the network security model produced allows an analyst or engineer to examine the system's security state at either micro or macro levels. Exact configurations can be examined if needed, or big-picture analysis of system interdependencies and relations can be performed.

Models of the System Security Baseline can be consolidated by hand through diagramming or spreadsheet applications, or by using tools commonly associated with Security Risk Management, Security Compliance, and Network Communications Modeling and Simulation. Such tools are designed to collect discrete details of system and network configurations, and provide validation that systems are configured according to established security standards. However, they prove very useful for building system security baselines for deep analysis.

2.2.1 Network Security Modeling and Simulation

Network Security Modeling and Simulation focuses on known vulnerabilities and relationships between vulnerable systems, and relies upon Security Risk Management or Compliance Validation tools to build system security baselines. Tools relied upon for network security modeling and simulation facilitate:

1. Consolidation of System Security Baselines
2. Organizational Exposure Analysis
3. Attack Vector Analysis
4. Allocation of Cost to Risk
5. Allocation of Mission to Systems

Using these models, system criticalities are analyzed and assigned to systems according to an organization's mission descriptions, continuity of operations plans, and other business plans. This represents an important stage in Cyber Effects Prediction as all analysis which follows will be dependant upon the completeness of the models and analysis produced at this point.

Traditionalists would argue that it is not accurate to use the term simulation in relation to how Security Risk Management tools allow an analyst to view systems. While the point can be argued at length, the important thing to understand is that the algorithms used by Security Risk Management tools analyze and quantify various security aspects of the system. This allows analysts to quickly differentiate between vulnerabilities that are reachable by cyber attack and therefore possess an elevated criticality.

2.2.2 Network Modeling and Simulation

While Network Security Modeling and Simulation addresses the link-node relationships between vulnerable systems that support attack vectors, Network Modeling and Simulation provides insight concerning system interdependencies. The basic premise of Network Modeling and Simulation within Cyber Effects Prediction is the identification of downrange (Secondary) effects resulting from the loss of systems and services hit by cyber attack. As such, system security baseline information used at this stage relates to more traditional network simulation of communications flow. The type of network analysis performed at this stage includes:

- Downrange Effects of Cyber Attacks
- Failover Analysis
- Bandwidth Consumption
- Overall Evaluation of the Exploit Environment

Networks are highly interdependent systems consisting of many tightly coupled services. As a result, cyber attacks can cause unexpected results. For example, the loss of an email server can not only result in the loss of email services for system users, it may also result in the loss or delay of sales personnel in capturing new business leads or submitting proposals against new business opportunities. Such a server does not necessarily have to be directly targeted for attack in this denial of service scenario.

Instead of exploiting vulnerabilities in the mail server itself, an attacker may choose to target the router which controls the Virtual Local Area Network (VLAN) in which mail servers reside. Likewise, an attacker could target areas of the infrastructures defense-in-depth in which mail gateways and mail content filters reside. In susceptible systems, the intended effect could be realized using these or similar targets. The analysis of downrange effects can also be enhanced through use of failover analysis or the analysis of bandwidth utilization to determine the resiliency of systems to cyber attack.

2.2.3 System Criticality

A system security baseline provides the technical details needed to describe the cyber battlefield on which an organization must fight. However, by itself a system security baseline does not reflect the importance of specific systems to an organization's mission or operations.

Standard business practice should generate documentation that can be used to overlay system criticality onto the system security baseline. This can be accomplished by labeling assets, or otherwise tagging assets within the system security baseline with descriptions which provide weight for measuring system criticality. If the organization has not clearly defined system criticality, an analyst must derive appropriate weights from the available documentation. Business products that may provide insight for assigning system criticality to a system security baseline may include:

- Mission Statements and Plans
- Organization Charts
- Risk Assessments
- Continuity of Operations Plans
- Corporate Phone Listings

2.2.4 Organizational Exposures

Organizational exposures refer to vulnerable or mis-configured hosts, servers, and network devices that serve as entry points for cyber attacks on information systems. These entry points may either reside at the perimeter of an information system, or at a less obvious internal points of origin.

The most important data point needed to perform exposure analysis is a verified and reliable system security baseline, a snapshot of a network's security state at a specific point in time. If constructed from valid data, a reliable representation of vulnerabilities and their associated severities can be presented in relation to network topology and configuration.

Organizational exposures should not be confused with attack sources. With the exception of some forms of Internal organizational exposures, many attacks originate from outside either the physical or logical perimeters of an information system. Corresponding to any organizational exposure is a cyber threat, which can be described in terms of actors and methods which present the potential to exploit a given organizational exposure.

2.2.4.1 Internal Exposures

Internal Organization Exposures are characterized by the physical interfaces through which cyber attacks may pass. Internal Organization Exposures require direct access to information systems, and are performed by either knowing or unknowing actors. As the technical means exposures are closed within well configured networks, attackers shift to the weakest security link in a given target system, its users.

Attempts to compromise internal organization exposures focus on gaining access to computing resources, and may include:

- User Interaction
    - Direct use of Keyboard, Mouse
    - Indirect replay of User Activity from scripted actions, key-loggers, mouse-loggers
- Introduction of External Media and Communications
    - Optical Disks
    - Magnetic Media
    - Thumb Drives
    - Rouge Wireless Access Points
    - Smart Phones
- Theft
    - Desktops / Laptops
    - Mobile Devices
    - User Badges / Security Tokens
    - Removable Media
- Social Engineering
    - Interviewing
    - Enticements
    - Unauthorized Entry
    - Footprinting

2.2.4.2 External Exposures

External organizational exposures represent vulnerabilities at network perimeters, which allow access to internal systems once exploited. These can be identified through authoritative vulnerability scanning of perimeter devices, with the analytical assumption that any perimeter device possessing vulnerabilities

that can provide an attacker administrative access can allow attack propagation further into network infrastructures.

This category of exposure acts as a hop-point for network based attacks to enter protected infrastructures from the internet, and may take advantage of weakly configured or non-hardened systems, such as:

- Routers
- Firewalls
- Intrusion Detection / Prevention
- Mail Routers
- Data Guards
- Content Filters
- Other edge protection or routing devices

2.2.4.3 Hybrid Exposures

Hybrid Exposures take advantage of Internal Exposures to facilitate the exploitation of External Exposures from within protected infrastructures. These exposures may originate from the intentional mis-configuration of systems by privileged users to circumvent security controls from within networks, or the negligent use of Internet or E-Mail resources resulting in the introduction of malicious code. Often the malicious code introduced will execute reverse shells which initiate access for attackers to otherwise protected systems.

2.2.5 Cyber Attack Vectors

Advanced security analysis techniques build upon exposure analysis to align known vulnerabilities with the potential effects of their exploitation. With the knowledge of which exploits allow compromised systems to be used as jumping off-points to critical systems deeper within a network infrastructure, routes can be identified that an attacker could potentially use to infiltrate the network. This information represents potential attack vectors, from which organizational exposure to cyber threats can be defined.

Cyber attack vectors consist of the physical and logical paths a particular attack takes to reach its ultimate target, and allows for the identification of an organization's exposure to cyber threats as the result of thorough vulnerability analysis and the establishment of system security baselines. Through attack vector analysis using system security baselines, questions can be answered that vulnerability assessment alone is unable to address.

The basic process used to perform the degree of analysis needed consists of three phases, which includes:

a. Use information security modeling and simulation tools to generate a system's security baseline configuration based on network device configurations, firewall rules, and vulnerability scans.

b. Harness system security baselines to provide the elements of information needed to build a composite view of potential attack vectors representing an organization's exposure to cyber threats.

c. Identify organizational exposure to cyber threats and facilitate the development of situational awareness by providing the information needed to effectively prioritize remediation actions while maximizing resource utilization of information security personnel, and budget.

2.2.5.1 Primary Cyber Effects

Primary Cyber Effects represent the impact to information systems from direct exploitation of vulnerabilities during cyber attack. Associated with Attack Graphing / Attack Vector Analysis. Includes analysis of Point-to-Point and Multi-Hop Attacks. Expands upon traditional vulnerability assessments by examining the link-node relationships between vulnerable systems. Focus is on vulnerabilities that could provide attackers sufficient access to target systems needed to "Own" the target system for use as an attack platform

2.2.5.2 Secondary Cyber Effects

Secondary Cyber Effects represent the indirect impact information systems experience when network services and communications are lost or restricted due to cyber attack. Indirect in nature, and consist of downstream effects of system failures triggered by cyber attack. Characterized as Internally Cascading Effects that occur within systems. Exploits the interdependency of networked services. Results from the failure of systems dependant upon those affected by direct attack or other internally cascading effects

2.2.5.3 Tertiary Cyber Effects

Tertiary Cyber Effects represent the overall impact of Primary and Secondary Effects which result in the loss or degradation Operational or Mission Capabilities that are external, yet dependant upon information systems. Characterized as Externally Cascading since Tertiary Effects occur outside of systems. Example… an obvious effect of financial systems failing can be employees not being paid, a non-obvious effect could be that logistics systems are unable to complete transactions.

2.2.5.4 Perform What-If Analysis…

Example – New Vulnerabilities are suspected in systems which are built on Operating System "A", running Application "B", with Service "C", and Port "D", exploitation allows administrative access. Modify Network Security Models to account for this new vulnerability, and re-work analysis. New Organizational Exposures and Attack Vectors may emerge depending upon the distribution of systems possessing vulnerable characteristics.

2.3 VULNERABILITY DEMONSTRATION

Penetration testing (pentest) may target analysis of either black box (unknown) or white box (known) systems. Cyber Effects Prediction lends itself to white box pentests, eliminating discovery since analysts possess a Network Security Model… aka System Security Baseline. Pentesting within this methodology is used to demonstrate and prove vulnerabilities that system owners may not otherwise acknowledge. Tools such as Metasploit or Core Impact are well suited to demonstrating targeted pentests against lab systems. Vulnerabilities exploited through custom developed code can be worked into Network Security Model based on attributes of systems and software targeted.

2.4 REMEDIATION AND RESIDUAL RISK

2.4.1 Prioritized Remediation

Vulnerability remediation can be a daunting task on any network, large or small. Technicians and engineers are trained that every vulnerability that is found must be fixed, yet are faced with decisions on how to implement fixes in production environments. Often problems are compounded as new alerts are released and additional remediation tasks are identified. By analyzing system security baselines for organizational exposures, mission criticalities, and attack vectors, those engineers and technicians responsible for implementing security measures can identify and fix systems that are most likely to suffer attack first.

Seeing as the vast majority of vulnerabilities within a given network are only reachable through indirect attack, the result is a reduction in the number of vulnerabilities requiring immediate remediation from thousands to hundreds, or even tens of critical vulnerabilities. However, if attack vector analysis is not performed, the systems which enable attack vectors likely go unidentified.

Taking the perspective that systems along attack vectors posses vulnerabilities that could be exploited and sufficient access be gained inherently hold the highest severity, initial remediation efforts can be focused on those direct exposures. A low rated vulnerability that is directly exposed to an attack vector may require elevation to high or critical. Likewise, a high rated vulnerability that is unreachable may represent a lower priority remediation.

2.4.2 Resource Allocation

Managing system security baselines for production systems is a laborious activity that can greatly impact the resources an organization has available for information systems management. Time, money, and personnel must be allocated away from other operationally focused activities to ensure that systems are not compromised, and to remediate any potential compromises that may have occurred. As a result, shortcuts may be taken when managing system security baselines, if they are not neglected entirely.

In cases where complex, technically sophisticated attacks have compromised the security of an information system, significant impact to an organization's operations can occur as affected systems are brought down for intrusion response and remediation actions. An organization's cyber battle rhythm is then slowed as extended periods of degraded operational capabilities are realized while investigations move beyond known intrusions and analysis of other systems within a network. In some cases, complete system rebuilds are required to ensure that a known secure state is reached.

Cyber Effects Prediction allows efficient allocation of resources needed to conduct remediation actions, allowing the execution of time sensitive response actions. In the case of vulnerability remediation, organizations which perform this type of analysis are able to move to a proactive state where the truly critical issues are resolved first, allowing them to move to secure system baselines more rapidly.

Organizations are often hard pressed to fully patch systems or implement dynamic defense-in-depth strategies. Allocation of resources to remediate vulnerabilities is discretionary in nature, using Cyber Effects Prediction, resource allocation can be aligned with those vulnerabilities that are:

- Reachable
- Assigned to Mission Critical Systems
- Time Critical

- Proportionate to Resource Availability

2.4.3 Residual Risk

Proper use of attack vector analysis results in the modification of the severity reported by vulnerability assessment tools and the development of a credible assessment of those vulnerabilities. For example, a vulnerability reported by a scanner may be categorized by that tool as high or critical. This is because the vulnerability is reported by the tool out of context of the overall network security infrastructure. Were this vulnerability unreachable by potential attackers, it would still end up identified for immediate remediation using standard methodologies.

No approach to system security is perfect, and Cyber Effects Prediction is based on knowing your system security baseline and assessing it against published vulnerability databases. 0-day vulnerabilities can be worked into your network security model, and should be considered. Residual risk will remain that system owners will need to acknowledge and accept responsibility for. However, Cyber Effects Prediction provides a holistic view of System Security Baselines with an understanding of how mission critical systems may affected by cyber attack.

3 THE FUTURE OF CYBER EFFECTS PREDICTION

The ultimate impact of Cyber Effects Prediction is cost savings and avoidance through prioritizing the remediation of direct exposures. Repeatable processes for attack vector analysis are placed into the hands of the systems security engineers who need to provide timely and accurate information security analysis. Cyber Effects Prediction system owners can realize reduced network security development cycles, establish known good system security baselines, and increase overall network security states.

Cyber Effects Prediction today ranges from manual to semi-automated processes, to increase speed of analysis. However, integrated systems can be produced enabling a wider range of users to benefit. To do this product vendors should be engaged to integrate enabling technologies. Further, open source products can be tailored to better address attack vector analysis.

Other factors that will support the practice of Cyber Effects Prediction are the development of decision metrics which enable users to understand when analysis is good enough to act upon. Additionally, Cyber Effects Prediction must be decomposed into discrete, repeatable processes. Integrations of Systems for Cyber Effects Prediction into production environments which support near-real-time situational awareness is also needed.

System owners also require increased awareness of the benefits that can be derived from non-intrusive analysis provided by Cyber Effects Prediction. Development of this awareness can be supported through a portfolio of models and analysis that can be released to share with system owners, showing Cyber Effects Prediction in action.