IBM Security Services
Emergency Response Services from IBM
Help prepare for and withstand security breaches more effectively
Agenda

- Current market or industry situation
- Needs and challenges
- How the offering addresses needs and challenges
- Offering description
- Associated offerings
- Why IBM?
- Considerations and dependencies
- Next steps
Executive summary

- Today’s cyber attacks have become more sophisticated and more frequent—new technologies such as cloud, mobile devices and social media have virtually eliminated network boundaries and increased vulnerabilities.

- The lack of a unified incident management process, coupled with inexperienced staff, can increase the business impact of security incidents.

- To reduce these impacts, institute an enterprisewide threat prevention and response strategy that can not only assist you in recovering from unforeseen security breaches and downtime more quickly, but that can also prevent such incidents in the future.

- IBM Cybersecurity Assessment is designed to help:
  - Reduce risks and exposure to cyber threats through a more proactive and preventive approach
  - Provide access to key resources that can enable faster recovery and help reduce business impact from incidents
  - Enable a broader view and deeper understanding of incidents using intelligence data and analytics

- IBM leverages the expertise of our industry certified analysts and consultants who have specialized experience in various technical fields across industries.
Here is a chronological illustration of the potential events involved in a hypothetical security incident scenario.

**7:00AM**
An Asian utility company experiences network latency—suspicious traffic is discovered on their network.

**8:00AM**
Unknown malware attacks are detected as generating from the traffic—causing disruption to business operations.

**12:30PM**
The hackers attack internal systems and steal sensitive data.

**2:30PM**
The incident response team struggles to restore services—the attack replicates to business partners.

**5:00PM**
Real-time applications are down and production databases are lost.

**7:00PM**
The lack of a unified and tested incident response process renders every attempt to recover from the attack unsuccessful.
The effects of a single security incident can prove to be devastating to the business.

In a security incident scenario, there could be multiple damages within 12 hours of the attack:

- Claims that cyber attackers are taking down the organization are spreading throughout media channels
- Sensitive client information is posted to public domains
- Password list is stolen and made public
- Production databases have been deleted
- Internal communications and most applications are down
- Design documents and source codes of the company’s flagship products have been stolen
- Business partners are affected by the attack
- The organization’s reputation is in jeopardy
- Clients and business partners are angry and decide to terminate contracts
- Law enforcement and regulators start investigations
- There is a huge potential for financial loss
The preparation of cyber attackers may be much more elaborate than your preparation for the security incident.

- To prepare for the attack, thumb drives loaded with malware were planted around the corporate campus.
- Malware and backdoors were installed; command and control channels were set up.
- A spear phishing campaign was launched against key company individuals.
- Critical information, including system access credentials were stolen.
- Remote access Trojans were planted on internal workstations; command and control channels were set up in “stealth” mode.
- Significant effort was put into executing the attack with numerous groups.
The current trends indicate a radical shift in the security landscape.

1 Assuming a compromised environment

“One thing is clear: the longer a stealthy attacker sits undetected in the enterprise network and its endpoints, the more damage they can do.”

2 Most important capabilities become intelligence and response

“Our protection and prevention efforts should not be neglected, the true measure of an organization’s advanced persistent threat (APT) defenses is its ability to quickly detect breaches and thoroughly research the extent and impact of those breaches.”

2 IBM X-Force® 2012 Mid-year Trend and Risk Report
One of the ten security imperatives in 2013 is to upgrade incident response capabilities to prepare for advanced threats.

ICS-CERT incident response trends
Number of attacks reported and requiring onsite Help by US critical infrastructure companies

<table>
<thead>
<tr>
<th>Year</th>
<th>Incident response tickets</th>
<th>Incident response onsites</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>2010</td>
<td>41</td>
<td>8</td>
</tr>
<tr>
<td>2011</td>
<td>198</td>
<td>7</td>
</tr>
</tbody>
</table>

Source: ICS-CERT Incident Response Report, 2011

Relative maturity of IREC members’ incident response processes
Percentage of survey respondents at various maturity levels

Most organizations have outdated incident response capabilities; sophisticated attacks require chief information security officers (CISOs) to revisit their processes.

Source: 2013 Security Outlook November 2012, Information Risk Executive Council Study, Corporate Executive Board; Information Risk Education Council (IREC)
A security incident can adversely affect business operations, consumer trust and often have regulatory implications.

- **The threats are real**
  - Every sector of our economy has been affected by cyber attacks
  - Critical infrastructure is at risk
  - There has been 17-fold increase in infrastructure attacks from 2009 to 2011
  - You cannot stop an attack unless it is detected
  - There is an increased need to build a cyber radar

- **Sony Pegs PSN Attack Costs at US$170 Million**
  The Sony attacks in 2011 will cost it 14 billion yen (US$170 million dollars) in increased customer support costs, welcome-back packages, legal fees, lower sales and measures to strengthen security, part of a US$3.1 billion total loss in 2011.¹

- **In the event of a security breach, organizations need expert guidance to protect the availability of critical business systems—and to find and solve the root causes of the problem quickly.**

- **Vectors for attack are most often well-known vulnerabilities that should be addressed given a unified incident identification and management process.**

- **These issues and their resulting impact are easily preventable if organizations collaborated with a reliable security partner.**

¹Sony Pegs PSN Attack Costs at $170 Million, $3.1B Total Loss for 2011, Forbes, 2011.
Today’s threats (actors) are more sophisticated than ever.

<table>
<thead>
<tr>
<th>Threat</th>
<th>Profile type</th>
<th>Share of incidents</th>
<th>Attack profile</th>
</tr>
</thead>
</table>
| Advanced threat; mercenary     | ▪ National governments  
▪ Organized crime  
▪ Industrial spies  
▪ Terrorist cells                                 | 23 percent         | ▪ Sophisticated attacks  
▪ Espionage  
▪ Intellectual property theft  
▪ Systems disruption  
▪ Financial crime |
| Malicious Insiders             | ▪ Employees  
▪ Contractors  
▪ Outsourcers                                 | 15 percent         | ▪ Financial crime  
▪ Intellectual property theft  
▪ Unauthorized access |
| “Hacktivist”                   | ▪ Ethical and malicious hackers  
▪ “Protectors of internet freedom”                                    | 7 percent          | ▪ Inexperienced-to-higher-order skills  
▪ Target known vulnerabilities  
▪ Systems disruption – denial of service attacks  
▪ Web defacement  
▪ Information disclosure |
| Opportunist                    | ▪ Worm and virus writers  
▪ “Script kiddie”                                                | 49 percent         | ▪ Inexperienced or opportunistic behavior  
▪ “Acting for thrills” with limited funding  
▪ Target known vulnerabilities  
▪ Malware propagation  
▪ Unauthorized access  
▪ Web defacement |
| Other                          | ▪ Inadvertent insiders                                                | 6 percent          | ▪ No funding  
▪ Unwittingly cause malware outbreak and data loss  
▪ Through mobile access and social business |

An advanced, targeted attack can cause business disruption on multiple levels.

The anatomy of a targeted attack:
- Adversary compromises endpoint used by a systems administrator with undetectable malware
- Adversary impersonates the system administrator to gain privileged access to systems
- Data is stolen and production systems are further compromised
A denial-of-service (DDoS) attack can result in loss of business opportunities and brand image.

**Anatomy of a DDoS attack:**
- Adversary launches concurrent attacks from multiple worldwide locations
- Attacks intended to saturate network connections and disable web presence
There are definitive steps that you can take to help keep your organization safer.

To help protect your company from security failures, you should:

- Prioritize your risk
- Protect your company’s most valuable and vulnerable assets
- Prepare for the inevitable—and for worst-case scenarios
- Promote and support a culture of security awareness

However, organizations usually lack:

- A unified, cross-company policy and process for incident response
- Actionable insight and information act upon
- Incident management and forensic analysis tools for remote system capture and analysis
- Resources or skills to actively respond to and investigate security incidents
Lack of expertise and security skills can compound the risk to your data and infrastructure.

- **58** percent are unable to find people with the right skills.
- **53** percent complain of the inability to measure the effectiveness of their current security efforts.
- **66** percent struggle with an understaffed IT team.

81 percent of chief information security officer functions are re-organizing or have been re-organized within the last six months.\(^1\)

\(^1\)Corporate Executive Board, Information Risk Executive Council Study, July 2012
Our solution can provide near-real-time, on-site support to help identify, respond to—and—prevent security incidents more efficiently.

IBM Emergency Response Services can:

- Help reduce risks and exposure to cyber threats using a proactive and preventive approach
- Provide access to key resources that can enable faster recovery and help reduce business impact from incidents
- Enable a broader view and deeper understanding of incidents using intelligence data and analytics

We can offer an end-to-end to solution that includes multiple services on a subscription basis:

- Incident response, management and prevention
- Data acquisition and analysis
- Intelligence gathering
- Containment and eradication
- Recovery
- Better management of regulatory compliance
IBM Emergency Response Services are competitively priced.

- IBM Emergency Response Services is listed at US$42,000.

- The subscription also includes:
  - Initial onsite or remote kick-off and incident planning session
  - 120 staff hours per year, which can be utilized remotely or on site at your discretion for emergency response services or preventive services
  - Unlimited emergency declarations
  - Two seats on the IBM X-Force® Threat Analysis Service (additional can be purchased) backed by global intelligence research
  - Quarterly check point, remote support and update on threat landscape

- We also provide an hourly rate of US$375 as post-incident, ad-hoc support without a subscription.
Utilizing the 120 staff hours, IBM can perform one or multiple preemptive incident preparation services.

<table>
<thead>
<tr>
<th>Computer security incident response plan (CSIRP) gap assessment</th>
<th>Review current computer security incident response policy and processes; identify potential issues and update the plan accordingly.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active threat assessment</td>
<td>Evaluation of the current threat and risk level; identify malware or Botnet activities and other early signs of potential security attacks or advanced persist threats.</td>
</tr>
<tr>
<td>Incident response training and simulated exercise</td>
<td>Conduct a workshop to provide “first-responder” type training, followed by the run-through of a custom developed incident scenario or a tabletop “cyber war game”.</td>
</tr>
</tbody>
</table>
The IBM X-Force Threat Analysis Service can provide customized security intelligence and global insight about a wide array of threats.

As part of the solution subscription, the X-Force® Threat Analysis Service offers detailed analyses of global online threat conditions and includes:

- Up-to-the minute, customized security information about threats and vulnerabilities
- Expert analysis and correlation of global security threats
- Actionable data and recommendations that help you maintain your network security
We can deliver end-to-end response services across multiple stages.

<table>
<thead>
<tr>
<th>IBM Emergency Response Service (ERS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Kick-off and planning session:</strong> Conduct a one-day initial workshop to gather information, review current incident response plan and incident declaration process, discuss selection, scope and timing of preemptive services, and develop a service calendar</td>
</tr>
<tr>
<td><strong>2. Preemptive and readiness activities:</strong> Utilizing part of the subscription hours, provide gap assessment of your incident response plan; perform tabletop exercise based on a simulated attack scenario; and conduct active threat assessment to uncover existing threats</td>
</tr>
<tr>
<td><strong>3. Ongoing checkpoint and incident assistance:</strong> Ongoing checkpoints and threat review are conducted throughout the subscription on a quarterly basis; an assigned incident case manager or lead analyst is available for incident related advice and assistance</td>
</tr>
<tr>
<td><strong>4. Emergency incident support:</strong> IBM ERS has an around-the-clock standby team ready to respond to an emergency declaration; the emergency incident is reported by contacting the ERS hotline or the assigned case manager, who provides the initial triage</td>
</tr>
<tr>
<td><strong>5. Predictive and actionable threat intelligence:</strong> Access to IBM X-Force Threat Analysis Service (XFTAS) that evaluates global online threat conditions and provides analysis for proactive security management</td>
</tr>
</tbody>
</table>
Creating an automated and unified system can enable an enterprise to better monitor its operations.

There are steps that can be followed to institute a holistic incident management process in your organization:

- Build a skilled incident management and response team with sufficient resources to conduct the forensics required
- Develop a unified incident handling policy and process
- Leverage consistent tools and security intelligence for incident management and investigative forensics
IBM offers a suite of cyber security incident services that are supported by the cyber security intelligence and response team.

The cyber security intelligence and response team (CSIRT) is a global, elite team of security professionals responsible for providing services across geographies, commercial clients and outsourcing clients.

IBM offerings

We offer a wide range of cyber security incident services including:

- Incident response program
- Incident management
- Malware analysis
- Emergency response
- Penetration testing
- Application security assessment
- Application source code security assessment
Why IBM?

- **IBM Cybersecurity Assessment team:**
  - Our analysts and consultants are dedicated to incident response
  - We have resident malware specialists that can perform malware breakdown and behavioral analysis

- **Our teams work very closely with internal and external entities such as:**
  - The IBM X-Force® security research team
  - IBM Managed Security Services
  - IBM threat and intelligence team
  - IBM malware defense team
  - Information technology information sharing and analysis center (IT-ISAC) and financial services technology information sharing and analysis center (FS-ISAC)
  - InfraGard – a partnership between the Federal Bureau of Investigation (FBI) and the private sector
Why IBM? (continued)

- **Our consultants are former law enforcement, military and academic experts:**
  - Police detectives (child exploitation task force)
  - Special agents and forensic examiners
  - Department of defense cyber crime center (DC3)
  - Army criminal investigation division

- **They have authored books and papers on a variety of topics including:**
  - Cisco router forensics and hardening
  - Malware behavior patterns
  - Digital forensics and tools

- **They hold many certifications:**
  - Certified computer examiner (CCE)
  - Certified Information forensics investigator (CIFI)
  - Certified information security manager (CISM)
IBM has proven security consultancy practices and dedicated security research capabilities across the globe.

IBM research

- 10 billion analyzed web pages
- 150 million intrusion attempts, daily
- 40 million spam and phishing attacks
- 46 thousand documented vulnerabilities

Worldwide managed security services coverage

- Over 20,000 devices under contract
- Over 3,700 MSS\(^1\) clients worldwide
- Over 15 billion events managed per day
- Over 1,000 security patents
- 133 monitored countries (MSS)

\(^1\)MSS - Managed security services
IBM has one the largest and most complex internal IT infrastructures in the world.

- Over 2,000 major sites
- Over 170 countries
- Over 400,000 employees
- Approximately 200,000 contractors
- Over one million traditional endpoints
- Almost 50 percent of employees are mobile
Here is a use case scenario that shows how IBM can help companies develop a viable incident response plan.

In this example taken from a client engagement, a leading heart treatment center requested our services to help develop a computer security incident response plan (CSIRP) that also accounted for unique requirements such as Health Insurance Portability and Accountability Act (HIPAA) and existing IBM security offering services.

Solution:
IBM met with client executives to set expectations, understand the critical environment elements that required protection and understand what they had in place, if anything. We developed a CSIRP plan in partnership with the client that was accepted and approved by their chief executive officer (CEO).

Benefits:
- Going forward, the client has a viable plan in place to handle incidents of virtually any type
- IBM will continue to work with this client to test, update and develop their plan
This use case scenario provides an example of how IBM can help proactively identify malicious threats within your network.

In this example taken from a client engagement, a company that processes credit cards for 16,000 banks was experiencing a denial of service (DoS) attack and was concerned that it was a cover for something of a more malicious intent in their network. They asked IBM to help with the DoS attack and also to proactively scan their environment for other threats or sources of attack.

**Solution:**
IBM worked with the corporation at two different data centers to investigate the source of the DoS attack to investigate and scan the environment for potential threats.

**Benefits:**
- Potential damaging threats were identified and remediated before the client’s environment was exploited
This use case scenario illustrates how IBM can help assess and quantify the impact of malware infections.

In this example taken from a client engagement, IBM helped one of the world’s largest hotel companies understand the magnitude of an on-going malware infection and quantify the business impact for the chief financial officer (CFO) and chief information officer (CIO).

Solution:
- IBM suggested a new hybrid consulting approach consisting of security sales leaders, emergency response experts, security assessment practitioners and management consulting.

Benefits:
- Client’s immediate situation was contained and resolved
- Roadmap toward a higher level of security and future prevention was created with continued support from IBM for implementation
Trademarks and notes

IBM Corporation 2013

- IBM, the IBM logo, ibm.com, and X-FORCE, are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), these symbols indicate US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml

- Other company, product and service names may be trademarks or service marks of others.

- References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

- This document is current as of the initial date of publication and may be changed by IBM at any time.

- THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.