ISACA
Trust in, and value from, information systems
Denver Chapter

Exercising Your Enterprise Cyber Response Crisis Management Capabilities

Ray Abide, PricewaterhouseCoopers, LLP

Agenda

CEO view of cyber risks and recent statistics

Cyber risk disclosures

Cyber incident timeline

Cyber incident enterprise impact

Business continuity management definitions and benefits

Legacy cyber incident exercises and the impacted enterprise

Cyber incident interruption scenarios to consider & exercise timeline

Some questions for management

CEO's view of cyber risks

69% of CEO's are concerned about IP/customer data protection, intellectual property protection, and cybersecurity.

In some industry sectors, cyber risk threatens growth. 71% of US CEOs in banking and capital markets cite cybersecurity concerns.

Companies are beginning to change how they think about cybersecurity—viewing it as a business issue, not an IT one.

Recent statistics

Financial Calculation

- Cybercrime is a tax on innovation, cost and jobs. It costs **$445 billion** each year in loss and clean-up

Cyber Monday

- **2014** Cyber Monday saw fewer attacks, but near record amounts of data stolen*

Protection

- Cybercrime and IT failure ranks in **Top 5** business risks for 1st time. There was an increase from 8th place in 2014 and 15th place in 2013**

Response and Remediation

- **78%** of CIO/CISO's have not provided a security strategy to their Board of Directors

Mobile

- Malware infection rates are now split 50/50 between Windows laptops and Android devices***

* IBM
**Kroll Ontrack
***Alcatel-Lucent

Cyber risk public disclosures

It is common place to see cyber-breach / cyber-attack disclosures in companies' 10-K SEC filings.

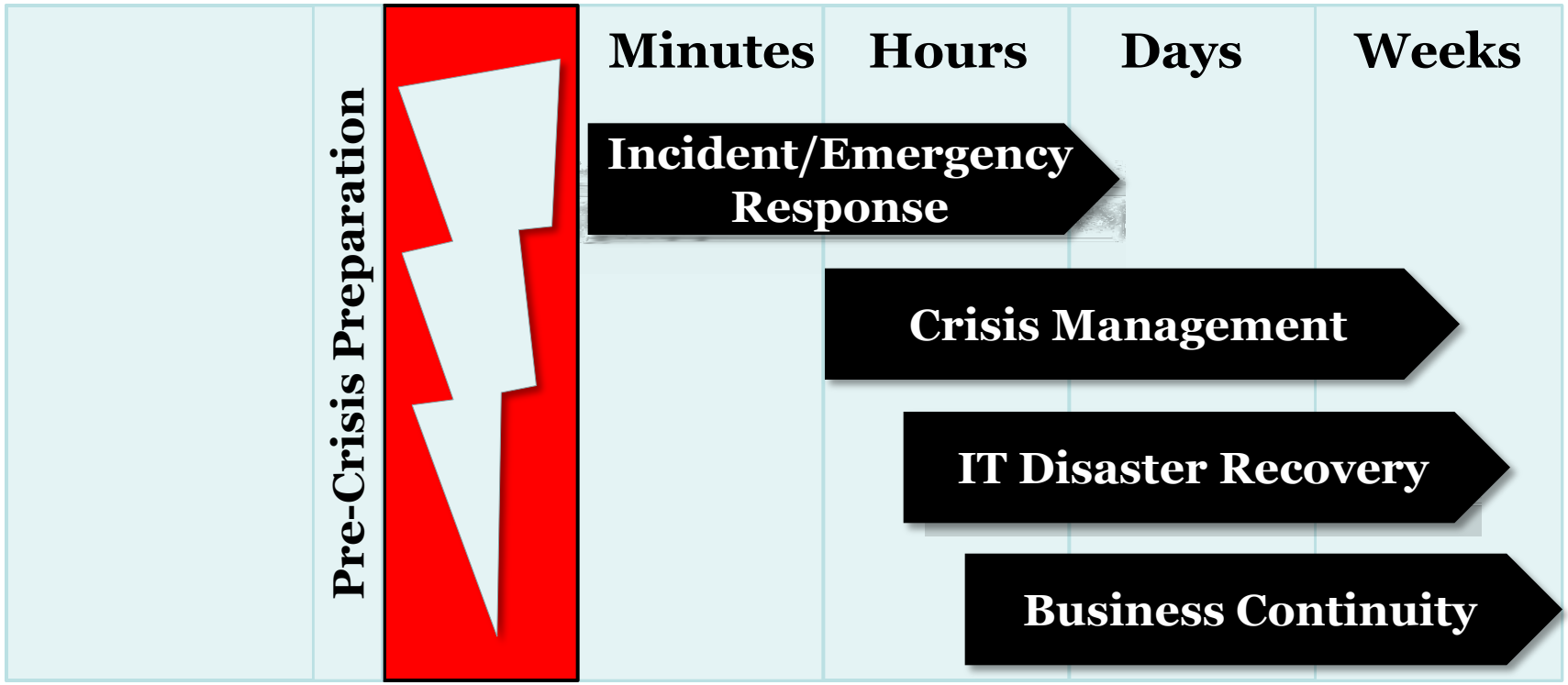
Any failure to maintain the security of the information relating to our customers, associates and vendors that we hold, whether as a result of cybersecurity attacks or otherwise, could damage our reputation with customers, associates, vendors and others, could cause us to incur substantial additional costs and to become subject to litigation, and could materially adversely affect our operating results. –

If our security measures are breached, or if our services are subject to attacks that degrade or deny the ability of users to access our products and services, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure. -

Increased cybersecurity requirements, vulnerabilities, threats and more sophisticated and targeted computer crime could pose a risk to our systems, networks, products, solutions, services and data. –

A cyber attack, information or security breach, or a technology failure of ours or of a third party could adversely affect our ability to conduct our business, manage our exposure to risk or expand our businesses, result in the disclosure or misuse of confidential or proprietary information, increase our costs to maintain and update our operational and security systems and infrastructure, and adversely impact our results of operations, cash flows, liquidity and financial condition, as well as cause reputational harm. –

Incident timeline



Cyber incidents have enterprise-wide impacts

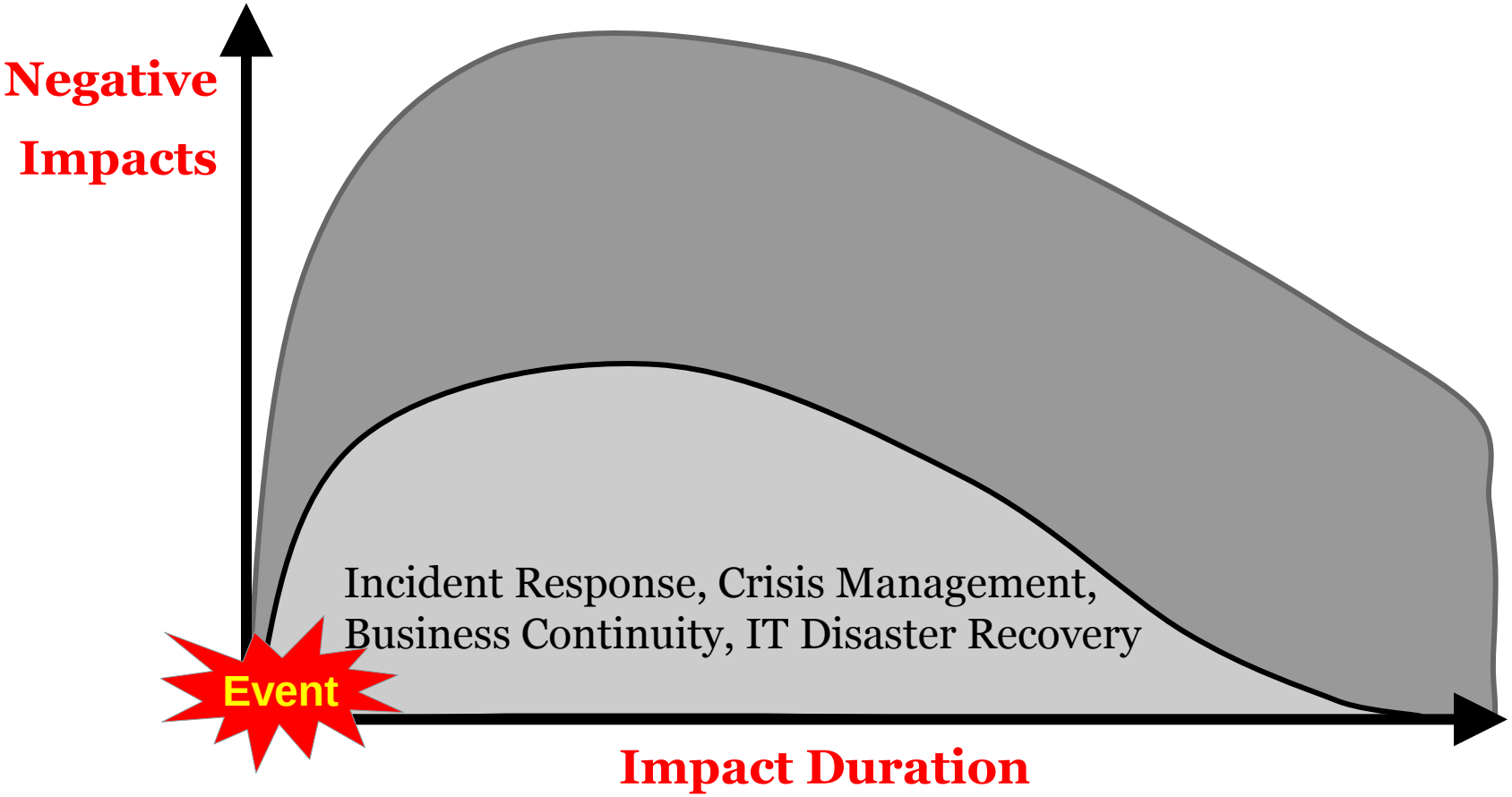
Financial, Operational, Reputation Impacts

- Interrupted and abandoned transactions
- Financial analyst and investor concerns result in value loss
- Supply/service chain interruption
- Loss of technology services
- Overwhelmed contact centers
- Unwelcomed media coverage
- Strained business relationships

Increased Costs

- Technology remediation
- Restoring brand
- Legal & regulatory
- Product redesign
- Advisors
- Compliance
- Insurance
- Training

Reducing the cyber incident's impact



Business continuity management defined

Business Continuity Management
Process of identifying, preventing, preparing for, and responding to, events that may disrupt business activities.

Crisis Management
Supports command and control during an operational disruption and includes incident identification, evaluation, escalation, declaration, plan activation and deactivation .

Incident / Emergency Response
Facilitates and organizes actions during emergencies. These involve procedures to protect personnel & assets.

IT Disaster Recovery
Addresses the restoration of business system software, hardware, IT infrastructure services and data during an incident.

Business Continuity
Addresses the recovery and continuity of critical business functions required to maintain an acceptable level of operation during an incident.

BCM can improve enterprise incident response

BCM program governance

BC/DR exercises

Program assessment

What risks could interrupt our operations?

How are these risks currently addressed?

How are critical processes impacted by service interruptions?

What resources do these critical processes rely upon to function effectively (technology, personnel, facilities, third parties)?

Which recovery strategies should be used?

Which strategies have worked previously?

Business Continuity Plans for critical processes

Crisis Management Plans

IT DR plan improvements

Legacy cyber incident exercises

Traditionally, cyber incident response exercises were often IT focused events.

Determine the what, how, where, and extent of breach.

Stop additional data loss or impact.

Take “infected” machines offline, but leave power on.

Initiate “clean” machines to take control

Ensure you won't infect the new machines

Summarize exercise results

Request additional cyber defense funding

Impacted enterprise

A cyber incident's impact often resonates throughout the organization

- IT
- Customer Care
- Internal External Communications
- Finance & Investor Relations
- Legal
- HR
- Supply / Service Chain
- Vendor Management
- Operations / Point of Service & Delivery

Cyber incident scenarios to consider

The following cyber incident exercise scenarios can easily be designed to exercise the enterprises crisis management plan:

Denial of Service attack – Customers and business partners unable to interact with the organization, fear of exposed data

Data Breach – Customer, patient, employee and IP data exposed and/or corrupted

Unplanned Outage of IT or Telecommunications – Denial of service turned inward, interrupting technology services, full-stop of critical operations

Loss of Key Supplier due to a cyber incident – Supply and service chain interruption, confidential IP exposed, other business partners concerned about their cyber exposure related to your vendor.

Example cyber table top exercise timeline

Act 1 – : unusual network activity detected that quickly overwhelms network and incapacitates applications. [IT Incident Response]

Act 2 – : Media reports breached data examples, customers unable to transact business, efforts to restore systems stability marginally effective, employees unable to access several key systems, stock price decrease. [IT Incident Response, Crisis Management, IT Disaster Recovery]

Act 3 – : Some systems restored and others remain unstable, media focus continues, revenue / order volume at lower levels, first lawsuit filed. [IT Disaster Recovery, Crisis Management, Business Continuity]

Example cyber table top exercise timeline

Act 1 – : unusual network activity detected that quickly overwhelms network and incapacitates applications. [IT Incident Response]

Act 2 – : Media reports breached data examples, customers unable to transact business, efforts to restore systems stability marginally effective, employees unable to access several key systems, stock price decrease. [IT Incident Response, Crisis Management, IT Disaster Recovery]

Act 3 – : Some systems restored and others remain unstable, media focus continues, revenue / order volume at lower levels, first lawsuit filed. [IT Disaster Recovery, Crisis Management, Business Continuity]

Questions for management

1. Have you discussed cyber security risks with your audit committee?
2. Does your company have a comprehensive internal audit plan for your company's cyber security program?
3. How well was your business continuity plan designed to respond to cyber incidents?
4. If cyber threats present a significant risk to the organization, has a crisis management table top exercise been conducted using a cyber incident scenario?
5. If a cyber incident response has been exercised, was the business impact analysis used to identify exercise participants based on interrupt impact?
6. Has the organization determined how it will respond to one of their key vendors being impacted by a cyber incident resulting in their product / service interruption?
7. Does your company have a cyber security program and has your company assessed it using the federally issued preliminary cyber security framework?
8. What company assets are most vulnerable to cyber attacks?
9. Does your company have an cyber incident response plan? And is that plan updated and tested periodically?