นโยบายและการพัฒนาด้านเทคโนโลยีสารสนเทศเพื่อใช้กำกับให้สอดคล้องกับกฎหมายและมาตรฐานสากล

บรรยายโดย: นายชัชวาล บุญแต่ง

CAT Telecom Public Company Limited.

บริษัท กสท โทรคมนาคม จำกัด (มหาชน) CAT TELECOM PUBLIC COMPANY LIMITED
http://www.cattelecom.com

CAT cyfence
Securing your Digital Assets

Agenda

- นโยบายด้านความมั่นคงปลอดภัยของระบบเครือข่ายและสารสนเทศ
- ระบบบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่ายภายในหน่วยงาน
- การกำกับดูแลด้านความมั่นคงปลอดภัยระบบเครือข่ายและสารสนเทศ

CAT cyfence
Securing your Digital Assets

Agenda

- กฎหมายที่เกี่ยวข้อง
  - พรฎ. ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ 2553
  - พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
  - กพร. การพัฒนาคุณภาพการบริหารจัดการภาครัฐ
- มาตรฐานอ้างอิง
- การพัฒนาบริหารจัดการระบบสารสนเทศและการกำกับดูแล
- Site Reference

CAT cyfence
Securing your Digital Assets

กฎหมายที่เกี่ยวข้อง

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ปี 2544

คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

บังคับใช้

พระราชกฤษฎีกา
กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ปี 2549

มาตรา 5 , 7 , 8

- มาตรา 5 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Access Control, Backup/Contingency, Risk Assessment)
- มาตรา 7 ให้ความเห็นชอบนโยบาย
- มาตรา 8 จัดทำตัวอย่างแนวนโยบาย

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศของหน่วยงานภาครัฐ ปี 2553
(นโยบายต้องประกอบด้วยอะไรบ้าง? ตามมาตรา 8)
Contingency Plan & IT Risk Assessment

พระราชกฤษฎีกา
ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ ปี 2553
(มาตรฐานในการให้บริการ IT)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ 2550

CAT cyfence
Securing your Digital Assets

(กพร.) การพัฒนาคุณภาพการบริหารจัดการภาครัฐ

ส่วนราชการจะต้องมีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ

ความคาดหวังจาก กพร.

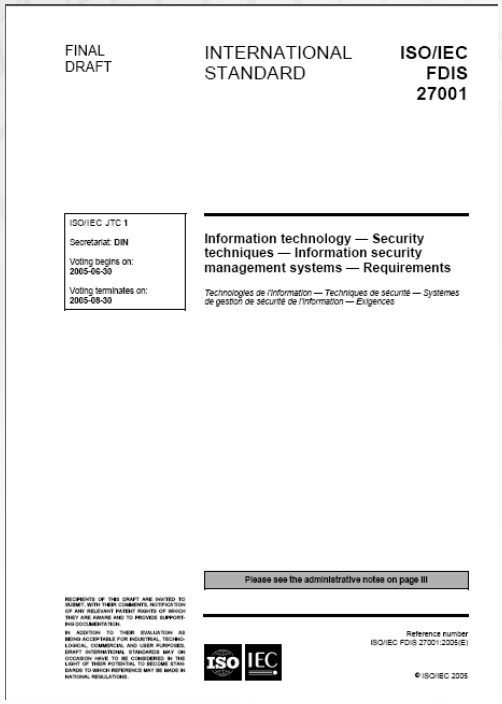
Policy

- **Access Control**
- **Backup (DR-site)**
- **Contingency Plan**
- **Audit (November,2011)**

CAT cyfence
Securing your Digital Assets

มาตรฐานอ้างอิง

- **มาตรฐาน ISO/IEC 27001:2005**
- มาตรฐาน ISO/IEC 17799
- **มาตรฐานการรักษาความมั่งคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550**
- มาตรฐาน BS 25999-1 / BS 25999-2


FINAL DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 27001

ISO/IEC JTC 1
Secretariat: DIN
Voting begins on: 2005-08-30
Voting terminates on: 2005-08-30

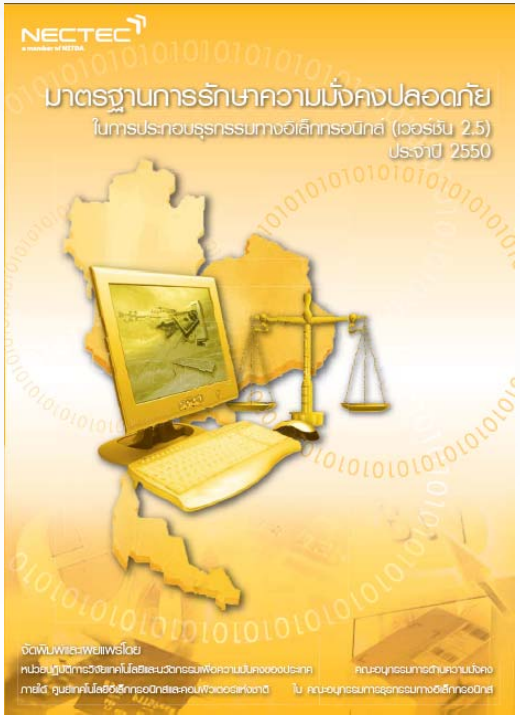
Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de gestion de sécurité de l'information — Exigences

Please see the administrative notes on page III

Reference number
ISO/IEC FDIS 27001:2005(E)

© ISO/IEC 2005




BS 25999-1:2006

BRITISH STANDARD

Business continuity management –

Part 1: Code of practice

BSI
British Standards

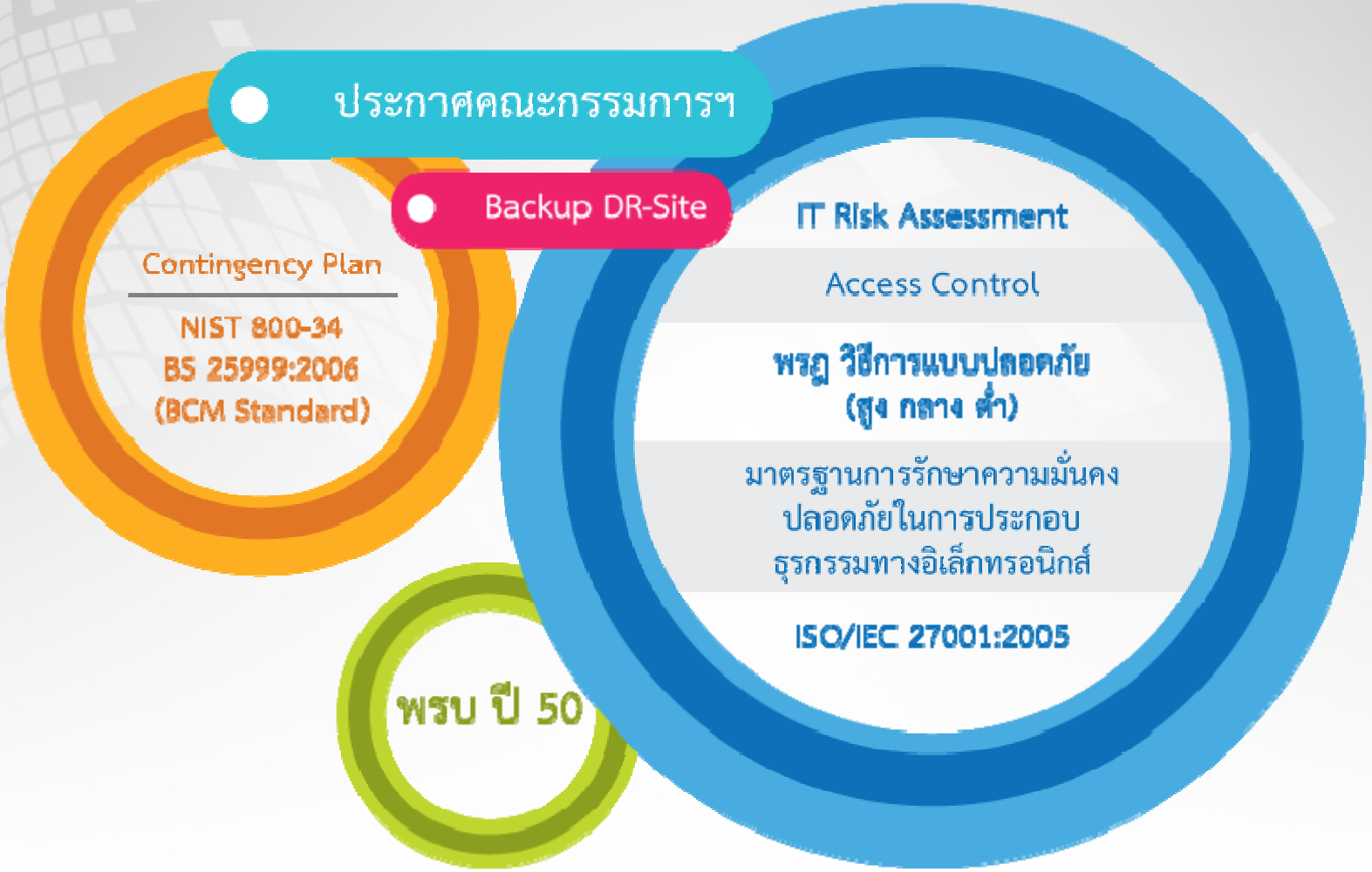
CAT cyfence
Securing your Digital Assets

มาตรฐานอ้างอิง

สาระสำคัญของมาตราฐาน ISO/IEC 27001 และ ISO/IEC 17799 ฉบับประเทศไทย (เวอร์ชั่น 2.5) ประจำปี 2550	
1.นโยบายความมั่นคงปลอดภัย (Security Policy)	**6.การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร** (Communication and Operations management)
2.โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Internal Organization)	**7.การควบคุมการเข้าถึง** (Access Control)
3.การบริหารจัดการทรัพย์สินขององค์กร (Asset Management)	**8.การจัดหาการพัฒนาและการบำรุงรักษาระบบสาสนเทศ** (Information Systems Acquisition, Development and Maintenance)
4.ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคคลากร (Human Resources Security)	**9.การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร** (Information Security Incident Management)
5.การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)	**10.การบริหารความต่อเนื่องในการดำเนินงานขององค์กร** (Business Continuity Management)
	11.การปฏิบัติตามข้อกำหนด (Compliance)

CAT cyfence
Securing your Digital Assets

มาตรฐานอ้างอิง



CAT cyfence
Securing your Digital Assets

การพัฒนาระบบสารสนเทศ

- **Policy**
- **Risk Assessment**
- **Contingency & DR Site**

CAT cyfence
Securing your Digital Assets

Policy

แนวนโยบาย

- การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
- จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน
- จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง
- การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

นิยาม

- ผู้ใช้งาน
- สิทธิของผู้ใช้งาน
- สินทรัพย์
- การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
- ความมั่นคงปลอดภัยด้านสารสนเทศ
- เหตุการณ์ด้านความมั่นคงปลอดภัย
- สถานการณ์ด้านความมั่นคงปลอดภัย ที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

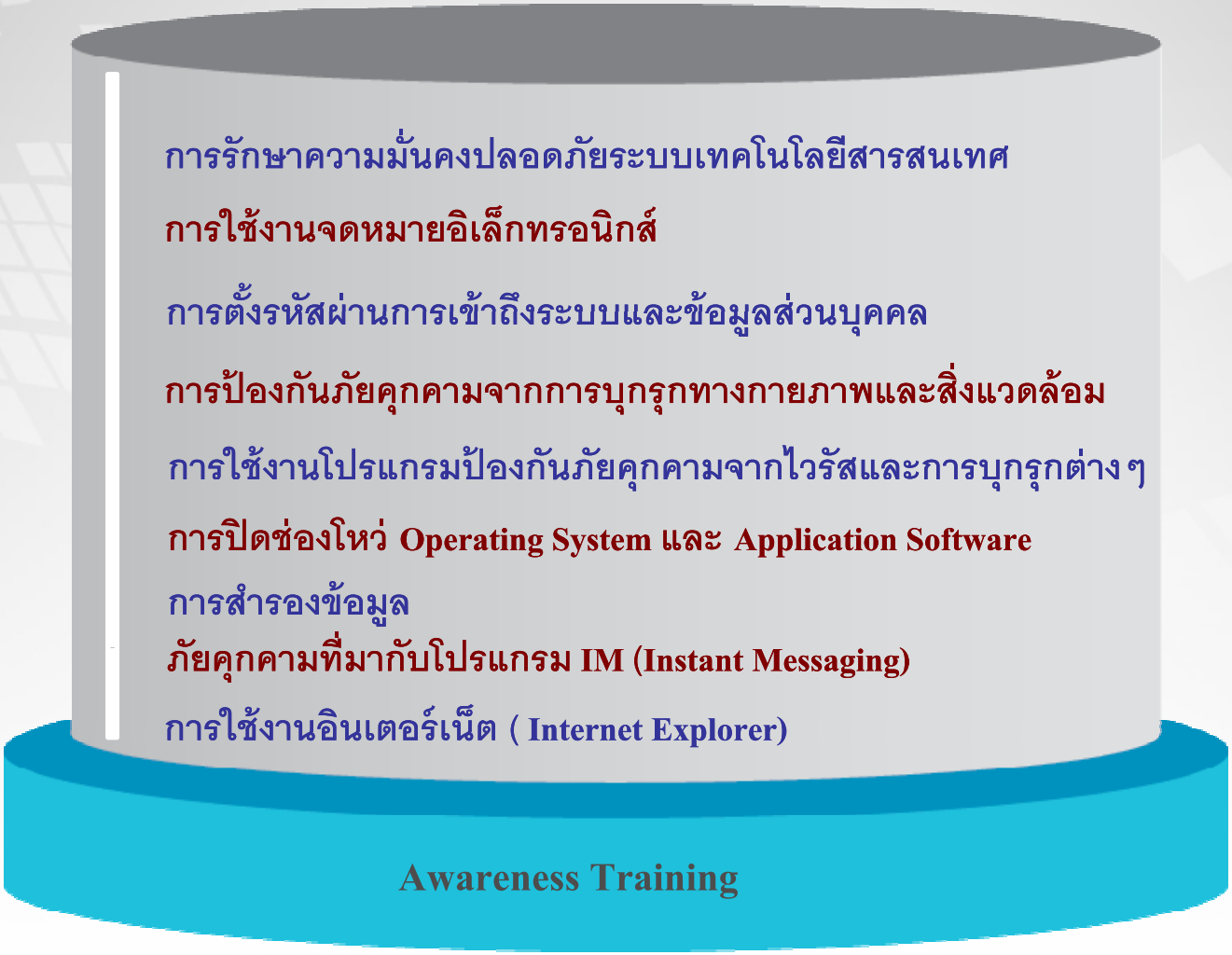
CAT cyfence
Securing your Digital Assets

Policy

แนวทางปฏิบัติ

CAT cyfence
Securing your Digital Assets

Basic Policy



CAT cyfence
Securing your Digital Assets

Guideline for Security Audit

รูปแบบดำเนินการตรวจสอบ

- Open Source Security Testing Methodology Manual (OSSTMM)
- Open Web Application Security Project (OWASP)
- Certified Ethical Hacker (CEH)
- Rapid7

https://www.owasp.org/index.php/Category:OWASP_Testing_Project

http://www.eccouncil.org/certification/certified_ethical_hacker.aspx

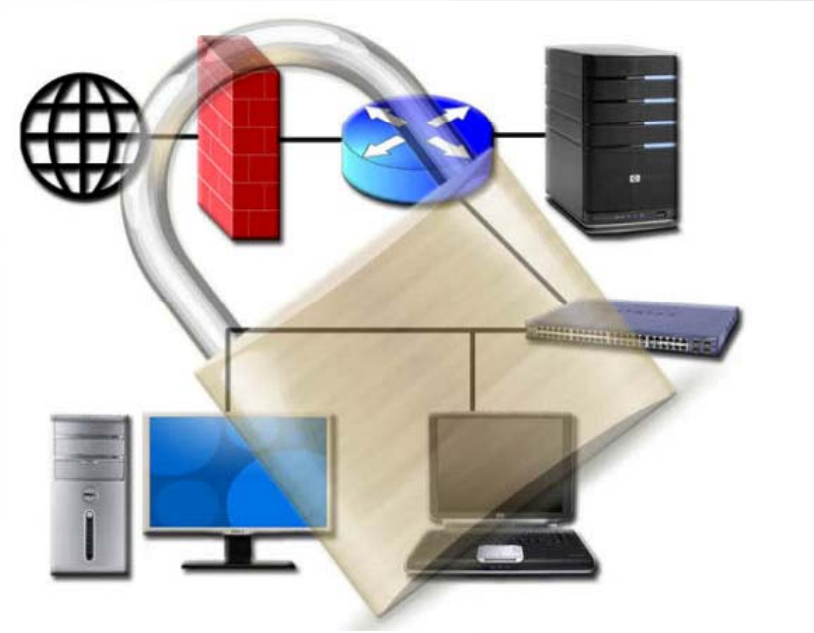
http://www.rapid7.com/company/

http://www.gartner.com/technology/about/policies/usage_guidelines.jsp

IT Risk Assessment

Action

- Vulnerability Assessment
- Penetration Test



CAT cyfence
Securing your Digital Assets

IT Risk Assessment

Vulnerability Assessment

ให้คำแนะนำพร้อมรายงานสรุปผลการวิเคราะห์และการประเมินความเสี่ยงของช่องโหว่ เพื่อให้องค์กรสามารถนำไปแก้ไขเพื่อการป้องกันและลดความเสี่ยงต่อภัยคุกคามระบบไอที

CAT cyfence
Securing your Digital Assets

IT Risk Assessment

Penetration

External Scan

ทำการทดสอบการบุกรุกจากภายนอกองค์กร โดยจำลองการบุกรุกเข้าสู่เครือข่ายจากภายนอก ซึ่งจะมีการระบุช่วงวันและเวลาในการทดสอบการ บุกรุกก่อนที่จะดำเนินการทดสอบจริง

Internal Scan

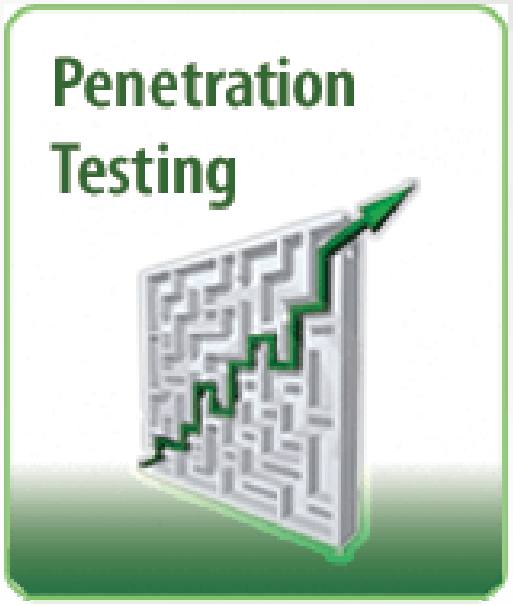
ทำการทดสอบการบุกรุกจากภายในองค์กร เพื่อทดสอบระดับความปลอดภัยของระบบจากการถูกเจาะระบบจากภายใน เสมือนผู้บุกรุกภายในองค์กร และค้นหาจุดเสี่ยงที่อาจเป็นอันตรายของระบบโดยรวม

CAT cyfence
Securing your Digital Assets

IT Risk Assessment

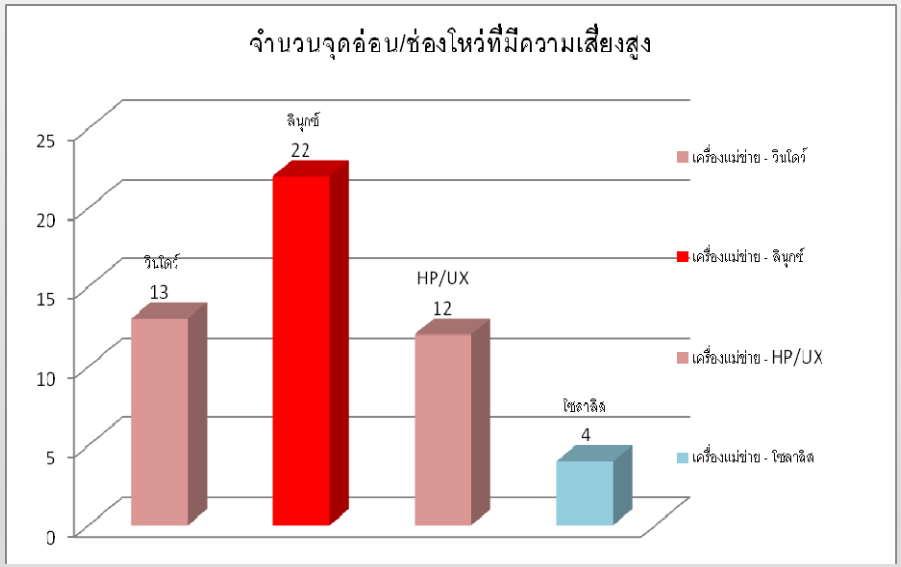
Penetration Test

- ทดสอบการเจาะระบบ Application & DB
- ทดสอบการเจาะระบบ Server & OS
- ทดสอบเจาะระบบ Network



IT Risk Assessment

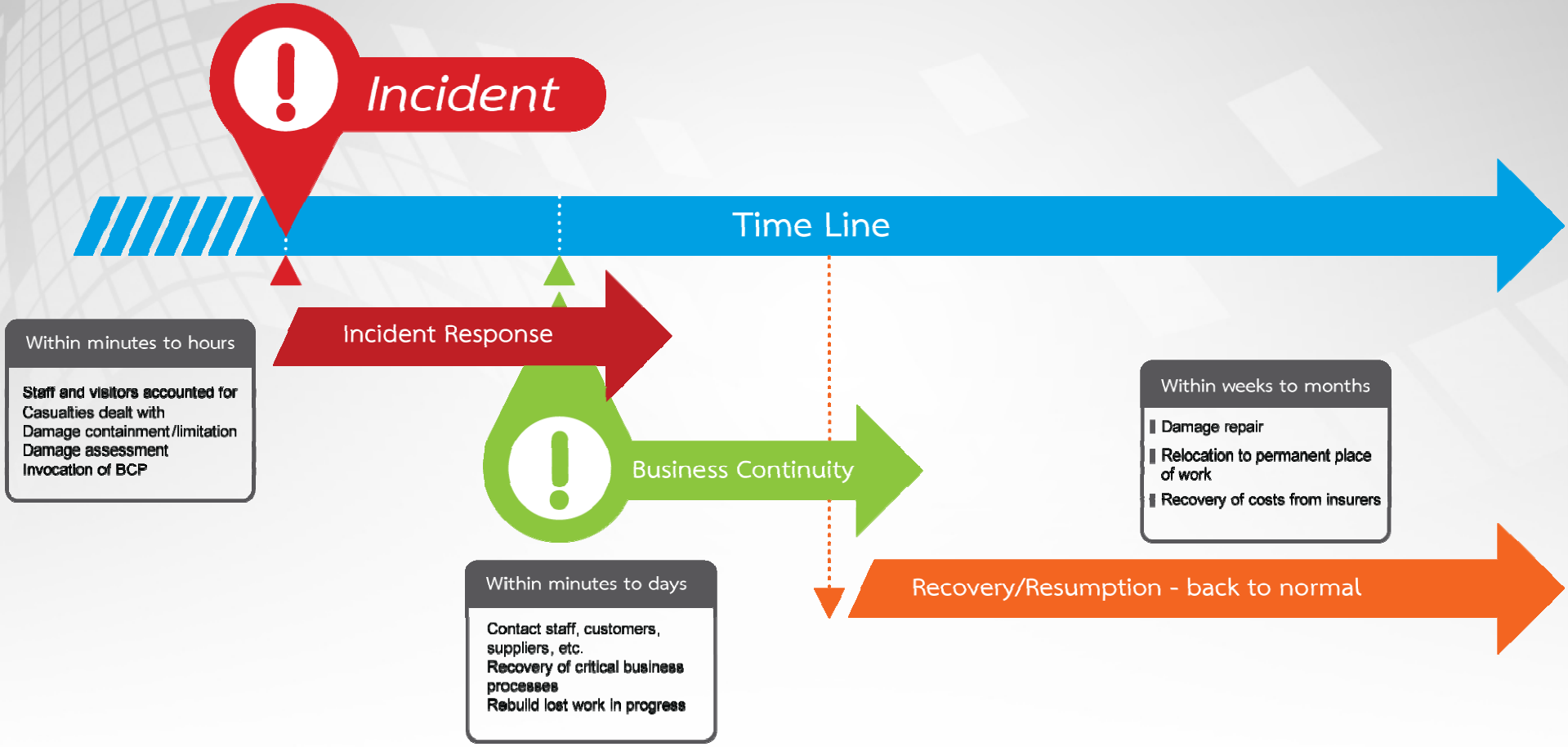
Benefit



- ภาพรวมด้าน IT Security ที่เป็นสถานการณ์ปัจจุบัน
- แนวทางการแก้ไข แนวทางการพัฒนาปรับปรุง การวางแผนงบประมาณ
- วัดผลความสำเร็จของการทำ IT Security

CAT cyfence
Securing your Digital Assets

Contingency Plan & DR Site



CAT cyfence
Securing your Digital Assets

Contingency Plan & DR Site

ขั้นตอนการดำเนินงาน (Procedure)

ตั้งทีมกอบกู้ภัยพิบัติ

การประเมินความเสี่ยงของการบริหารความต่อเนื่องทางธุรกิจ

วิเคราะห์ผลกระทบทางธุรกิจในการบริหารความต่อเนื่องทางธุรกิจ

จัดทำแนวทางรับมือภัยพิบัติ

ทดสอบแผนภัยพิบัติ

CAT cyfence
Securing your Digital Assets

Contingency Plan & DR Site

DR Site

- In House
- Outsource

CAT cyfence
Securing your Digital Assets

ประโยชน์ที่ได้รับ

- ระบบสารสนเทศที่มีความมั่นคงปลอดภัย
- แผนการพัฒนาระบบเทคโนโลยีสารสนเทศที่เป็นรูปธรรม
- ระบบสารสนเทศที่มีมาตราฐานการปฏิบัติงาน
- แผนภัยพิบัติฉุกเฉินที่มีประสิทธิภาพ
- มาตราฐานและระบบการดำเนินการที่ชัดเจนเป็นขั้นตอน
- มีสัดส่วนความรับผิดชอบตามกรอบหน้าที่อย่างชัดเจน

CAT cyfence
Securing your Digital Assets

บริการที่ CAT

IT Security
Professional Services

- IT Risk Assessment
- Security Solution
- CCTV Solution

Internet Security

- Email Security
- Secure Mail Hosting
- Web Security
- All@Secure
- Secure Remote Access

Secure Log Management

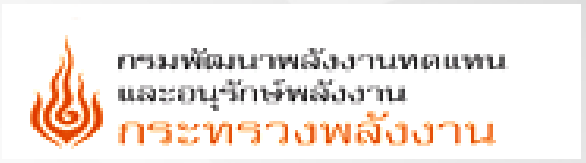
- Secure Log Management
- SmartLog

Managed Security Service

- Managed Security Service

CAT cyfence
Securing your Digital Assets

Site Reference



CAT cyfence

Securing your Digital Assets

ขอขอบคุณผู้ร่วมฟังบรรยายทุกท่าน

บริษัท กสท โทรคมนาคม จำกัด (มหาชน) CAT TELECOM PUBLIC COMPANY LIMITED

http://www.catcyfence.com