“TREND KEYWORD 2026”

HAVE

MFA (Multi-Factor Authentication)
ในบริบทของ MFA "Have" หมายถึง ปัจจัยการแสดงตัวตน (Authentication Factors) ซึ่งแบ่งออกเป็น 3 กลุ่มหลัก คือ:

สิ่งที่คุณ **รู้**:
ข้อมูลที่มีแค่คุณที่จำได้ เช่น รหัสผ่าน (Password), PIN, คำถามยืนยันตัวตน

สิ่งที่คุณ **ครอบครอง**:
อุปกรณ์ทางกายภาพหรือดิจิทัล เช่น โทรศัพท์มือถือ การรับ SMS, OTP, แอปพลิเคชัน Token (Google Authenticator),บัตร Smart Card หรือ USB Key (YubiKey)

สิ่งที่คุณ **เป็น**:
ข้อมูลทางชีวภาพ (Biometrics) เช่น ลายนิ้วมือ, การสแกนใบหน้า, การสแกนรูม่านตา

มีการยืนยันตัวตนต้องมีอย่างน้อย 2 ปัจจัยขึ้นไป

มีการแจ้งเตือนเมื่อมีการพยายาม Login

MFA

DO NOT HAVE

ในเชิงความปลอดภัย "Do not have" หรือสิ่งที่ ไม่ควรมี/ไม่ควรเกิดขึ้น เพื่อให้ระบบ MFA แข็งแกร่ง คือ:

No Single Point of Failure:
ไม่มีช่องโหว่เพียงจุดเดียว เช่น ระบบต้องไม่มีช่องโหว่ที่ทำให้การทำงานหยุดชะงักทั้งหมด
ตัวอย่าง: หากคุณมีเพียงรหัสผ่านโดยไม่มีการยืนยันผ่านโทรศัพท์มือถือ คุณจะไม่สามารถเข้าถึงระบบได้ (เพื่อป้องกันกรณีที่รหัสผ่านรั่วไหล)

No Static Access:
ไม่ควรมีการเข้าถึงแบบ "ถาวร" โดยไม่ตรวจสอบซ้ำ เมื่อมีการเปลี่ยนอุปกรณ์หรือเปลี่ยนสถานที่

No Sharing:
OTP หรือ ลายนิ้วมือ ต้องไม่สามารถแบ่งปันหรือส่งต่อให้คนอื่นได้โดยง่าย

No Dependency on Password alone:
ไม่พึ่งพาแค่รหัสผ่านเพียงอย่างเดียว เพราะรหัสผ่านเป็นสิ่งที่ถูกดักจับหรือคาดเดาได้ง่ายที่สุด

NO VPN

ความเสี่ยงของ SSL VPN (หรือ Web VPN) ในปี 2024-2025 ถือเป็นประเด็นร้อนแรงมากในวงการไซเบอร์ เนื่องจากเป็นช่องโหว่ยอดนิยมที่กลุ่ม Ransomware และ Hacker เลือกใช้เป็นอันดับต้น ๆ

RISKS IT HAS	Protections it does NOT HAVE
ความเสี่ยงที่แฝงมากับโครงสร้างของ SSL VPN เอง	สิ่งที่ SSL VPN ไม่สามารถป้องกันได้ หรือขาดไปเมื่อเทียบกับระบบใหม่อย่าง Zero Trust Network Architecture (ZTNA):
• **Have Critical Vulnerabilities** (มีช่องโหว่ร้ายแรงบ่อย): ในช่วงปี 2024-2025 มีการพบช่องโหว่ประเภท RCE (Remote Code Execution) ในอุปกรณ์ยี่ห้อดัง เช่น Fortinet, SonicWall, Ivanti ที่เปิดทางให้ Hacker เข้าควบคุม Firewall ได้โดยไม่ต้องใช้รหัสผ่าน	• **No Continuous Verification** VPN ส่วนใหญ่ตรวจสอบตัวตนแค่ตอน Login ครั้งแรกแต่ไม่มีการตรวจสอบซ้ำระหว่างการใช้งาน หากSession ถูกขโมย Hacker จะสามารถใช้งานได้จนกว่าจะหมดเวลา Login
• **Have Implicit Trust** (มีความเชื่อใจที่มากเกินไป): เมื่อ User ผ่านVPN เข้ามาได้แล้ว มักจะได้รับสิทธิ์เข้าถึงทั้งเครือข่าย (Network-level access) ทำให้ Hacker ที่ขโมยรหัสมาได้สามารถ Lateral Movement โดยเป็นการย้ายตัวเองจากเครื่องหนึ่งไปอีกเครื่องหนึ่งได้	• **No Device Health Check** (ตรวจสอบในรุ่นพื้นฐาน): บ่อยครั้งที่ SSL VPN อนุญาตให้เครื่องที่ "ติดไวรัส" หรือ "ไม่ได้อัปเดต Patch" เชื่อมต่อเข้ามาได้ ทำให้มัลแวร์แพร่กระจายจากอินเทอร์เน็ตบ้านเข้าสู่อินเทอร์เน็ตสำนักงาน
• **Have Browser-Based Risks** การเข้าใช้งานผ่าน Browser (Clientless) ทำให้มีความเสี่ยงจากมัลแวร์ที่ฝังใน Browser เช่น Keystroke Loggers หรือการถูกดัก Session (Session Hijacking)	• **No Granular Application Visibility** ผู้ดูแลระบบมักจะเห็นว่า "ผู้ใช้ A ต่อ VPN อยู่" แต่ ไม่มีข้อมูลว่าผู้ใช้คนนั้นกำลังทำอะไรในแอปพลิเคชันบ้าง
• **Have Public Exposure** หน้า Portal สำหรับ Login ของ SSL VPN มักต้องเปิดสู่สาธารณะ ทำให้ถูกสแกนหาช่องโหว่หรือโดนโจมตีแบบ Brute Force (เดาสุ่มรหัส) ได้ตลอด 24 ชั่วโมง	• **No Protection against MFA Bypass** หาก Hacker ใช้ช่องโหว่หรือจุดอ่อนในระบบ (System exploit) พวกเขาจะสามารถข้ามขั้นตอนการตรวจสอบ Multi-Factor Authentication และเข้าถึงสิทธิ์ผู้ดูและระบบโดยตรงได้

ประเภทความเสี่ยง	SSL VPN
ช่องทางการโจมตี	สูง (เพราะเปิดหน้าเว็บให้ Hacker เห็นได้ง่าย)
ความรุนแรงของช่องโหว่	บ่อยและแรง มีช่องโหว่ระดับ RCE แทบทุกปี
การป้องกันมัลแวร์	ต่ำ (ถ้าใช้เครื่องส่วนตัวต่อเข้ามา)
ตัวอย่าง	CVE-2024-21762 (9.8 of 10) CVE-2024-55591 (9.6 of 10)

SIRT

SIRT Security Incident Response Team (SIRT/CSIRT): การสรุปแนวคิดสำหรับทีมตอบโต้เหตุการณ์ความมั่นคงปลอดภัย หรือ Security Incident Response Team (SIRT/CSIRT) คือการแยกแยะระหว่าง"ความพร้อมที่ต้องมี"กับ"ความล้มเหลวที่ต้องกำจัด" เพื่อให้รับมือวิกฤตไซเบอร์ได้อย่างมีประสิทธิภาพ ดังนี้

HAVE

ทีม SIRT ที่มีประสิทธิภาพสูงจำเป็นต้องมีองค์ประกอบ ดังนี้:

Have Clear Playbooks (มีแผนปฏิบัติการที่ชัดเจน): มีขั้นตอน (Step-by-step) สำหรับเหตุการณ์แต่ละประเภท เช่น Ransomware, Phishing, Data Leak เพื่อลดการใช้ "สัญชาตญาณ" แต่ให้เน้น "มาตรฐาน"

Have Visibility (มีทัศนวิสัยที่ดี): ต้องมีเครื่องมือที่สามารถมองเห็นสิ่งที่เกิดขึ้นในระบบได้ เช่น SIEM, EDR, Log Management หาก "มองไม่เห็น" ก็ "ไม่สามารถแก้ปัญหาได้"

Have Post-Incident Review (มีการถอดบทเรียน): ทุกครั้งที่จบเหตุการณ์ต้องมีรายงาน "Lessons Learned" เพื่อนำมาปรับปรุงระบบป้องกันให้ดีขึ้น

DO NOT HAVE?

สิ่งที่มักเป็นอุปสรรคหรือ "หลุมพราง" ที่ทีม SIRT ไม่ควรให้เกิดขึ้น:

No Finger-Pointing Culture (ไม่มีวัฒนธรรมการโทษกัน): เมื่อเกิดเหตุ ทีมต้องมุ่งไปที่การ "แก้ไข" ไม่ใช่หาคนผิด (Blame-free culture) เพื่อให้ข้อมูลถูกรายงานอย่างตรงไปตรงมา

No Communication Silos (ไม่มีการปิดกั้นข้อมูล): ข้อมูลต้องไหลลื่นระหว่างทีมวิเคราะห์และผู้บริหาร ไม่มีการกักข้อมูลไว้กับตัวจนทำให้การตัดสินใจผิดพลาด

No Single Point of Failure (ไม่มีจุดล้มเหลวเพียงจุดเดียว): ระบบหรือกระบวนการต้องถูกออกแบบให้ไม่มีองค์ประกอบใดที่ถ้าล้มเหลวแล้วจะทำให้ทั้งระบบหยุดทำงาน

No Ad-hoc Responses (ไม่ทำงานแบบไร้ทิศทาง): ไม่ตอบโต้หรือแก้ปัญหาเฉพาะหน้าไป วัน ๆ โดยไม่มีแผนรองรับระยะยาว

No Over-reliance on Tools (ไม่พึ่งพาเครื่องมือเพียงอย่างเดียว): เครื่องมือราคาแพงแค่ไหนก็ไม่มีประโยชน์ ถ้าไม่มีคนที่รู้วิธีอ่านค่าหรือวิเคราะห์เชิงลึก

ZERO TRUST

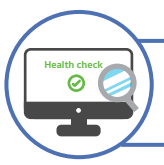
หากมี (Have) และไม่มี (Do not have) ระบบ ZTA (Zero Trust Architecture) จะมีความแตกต่างดังนี้

HAVE

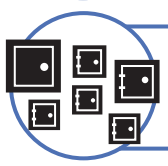
เพื่อให้บรรลุหลักการ "Never Trust, Always Verify" (ไม่เชื่อใจใครทั้งนั้น ต้องตรวจสอบเสมอ) ระบบต้องมีองค์ประกอบเหล่านี้:

Continuous Verification: มีการตรวจสอบต่อเนื่องไม่ใช่เพียงตอน Login ครั้งเดียว แต่ต้องตรวจสอบสิทธิ์และความปลอดภัยตลอดระยะเวลาที่ใช้งาน (Per-session basis)

Strong Identity (การมีตัวตนที่ชัดเจน): ต้องใช้ MFA (Multi-Factor Authentication) และตรวจสอบบริบทอื่นๆ เช่น Location, เวลาที่ใช้งาน, และพฤติกรรมของผู้ใช้



Device Health Check: มีการตรวจสอบสุขภาพของอุปกรณ์ก่อนให้เข้าถึงข้อมูล ต้องตรวจสอบว่าอุปกรณ์ที่ใช้อยู่มีการอัปเดต Patch ให้เป็น version ล่าสุดและมี Antivirusหรือไม่



Micro-segmentation: มีการแบ่งโซนย่อย แบ่งเครือข่ายเป็นส่วนเล็ก ๆ เหมือนมีห้องนิรภัยเล็ก ๆ อยู่หลายห้อง เพื่อป้องกันไม่ให้ Hacker ที่เจาะเข้ามาหนึ่งจุดได้ สามารถเจาะเข้าไปยังจุดอื่นได้ (Lateral Movement)

Least Privilege: มีสิทธิ์เท่าที่จำเป็นให้พนักงานสามารถเข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้องเท่านั้น (Just-in-time & Just-enough access)

DO NOT HAVE

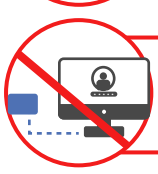
ถูกสร้างมาเพื่อกำจัดความเชื่อและช่องโหว่เดิม ๆ ดังนั้น สิ่งเหล่านี้จะ "ไม่มี" อยู่ในระบบนี้:

No Implicit Trust (ไม่มีความไว้วางใจโดยนัย): ผู้ใช้จะต้องไม่เชื่อว่าคนที่รู้จัก ปลอดภัยและเชื่อถือได้มากกว่าคนที่ไม่รู้จัก ระบบจะปฏิบัติกับทุกคนเหมือนกันและเท่าเทียมเสมอ

No Trusted Perimeter (ไม่มีขอบเขตที่เชื่อถือได้): ระบบจะไม่ถือว่าภายในเครือข่าย (Internal Network) ปลอดภัยโดยอัตโนมัติอีกต่อไป ทุกการเข้าถึงต้องได้รับการตรวจสอบไม่ว่าจะมาจากภายในหรือภายนอกองค์กร

No Permanent Access (ไม่มีสิทธิ์เข้าถึงแบบถาวร): ผู้ใช้หรืออุปกรณ์จะไม่ได้รับสิทธิ์เข้าถึงทรัพยากรตลอดไป แต่จะได้รับสิทธิ์ชั่วคราวตามความจำเป็น (Just-in-time access) และถูกเพิกถอนเมื่อไม่ใช้งาน เพื่อลดความเสี่ยงจากการถูกโจมตี

No Visibility Gaps (ไม่มีจุดอับสายตา): ต้องไม่มีส่วนใดของ Network ที่มองไม่เห็น (Dark Traffic) ทุกการเชื่อมต่อต้องถูกบันทึกและตรวจสอบ (Log & Monitor)



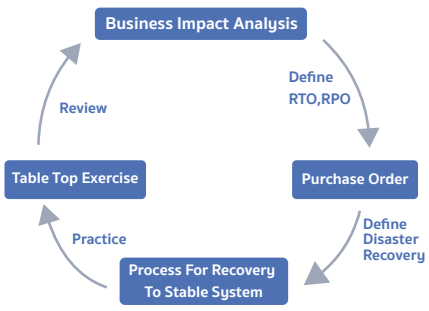
No Reliance on IP Address (ไม่เชื่อถือแค่ IP Address): ระบบจะไม่ถือว่า IP Address เป็นตัวบ่งชี้ความปลอดภัยหรือความน่าเชื่อถือ เพราะ IP สามารถถูกปลอมแปลงหรือใช้จากเครือข่ายที่ถูกเจาะได้

BCP

การจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) และแผนฟื้นฟูระบบคืนสภาพจากภัยพิบัติ (DRP) หรือเรียกว่ารวมกันว่า BCDR คือการเตรียมพร้อมเพื่อให้องค์กรอยู่รอดได้ในยามวิกฤต กล่าวโดยสรุปคือหากมี (Have) และไม่มี (Do not have) แนวคิด BCDR นี้ จะมีความแตกต่างดังนี้:

HAVE

เพื่อสู้กับวิกฤต เช่น ไฟไหม้, น้ำท่วม, ระบบโดน Ransomware ทีม BCDR ต้องมีองค์ประกอบเหล่านี้:



Have BIA (Business Impact Analysis): ต้องมีการวิเคราะห์ว่า "ถ้าส่วนนี้พัง องค์กรจะเสียหายกี่บาท" เพื่อให้รู้ว่าควรนำเงินไปลงทุนป้องกันส่วนไหนก่อน

Have Clear RTO & RPO:
RTO (Recovery Time Objective): จำเป็นอย่างยิ่งที่จะต้องกำหนดกรอบเวลาที่ชัดเจนสำหรับการกู้คืนระบบ เช่น ระบบจะต้องกู้คืนเสร็จสิ้นภายในกี่นาทีหรือกี่ชั่วโมง
RPO (Recovery Point Objective): ระยะเวลาสูงสุดที่องค์กรสามารถยอมรับการสูญหายของข้อมูลได้ เช่น หาก RPO ขององค์กรคือ 1 ชั่วโมง หมายความว่าองค์กรสามารถยอมรับการสูญเสียข้อมูลได้สูงสุด 1 ชั่วโมง

Have Tabletop Exercises (การซ้อมแผน): แผนที่ไม่เคยซ้อมคือกระดาษเปล่า ต้องมีการจำลองสถานการณ์และซ้อมปฏิบัติจริงอย่างน้อยปีละ 1-2 ครั้ง

Have Offsite Backups (3-2-1 Rule): ต้องมีข้อมูลสำรอง 3 ชุด โดยเก็บในสื่อ 2 ชนิด และมี 1 ชุดที่อยู่นอกสำนักงาน หรือบน Cloud

DO NOT HAVE

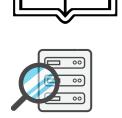
สิ่งที่มักเป็นจุดตายที่ทำให้แผน BCDR ล้มเหลวในสถานการณ์จริง:

No Theoretical Plans: ห้ามมีแผนที่ "เขียนสวยแต่ทำจริงไม่ได้" เช่น เขียนว่าให้ย้ายไปทำงานที่ตึก B แต่ตึก B ไม่มีอินเทอร์เน็ตเตรียมไว้

No Single Person Dependency: ความรู้เรื่องการกู้ระบบต้องไม่อยู่ที่เจ้าหน้าที่คนเดียว หากคนนั้นลาออกหรือติดต่อไม่ได้เมื่อเกิดเหตุขึ้น องค์กรจะต้องกู้คืนระบบได้ด้วยคู่มือการปฏิบัติงาน

No Obsolete Documents: ต้องมั่นใจว่าเอกสาร BCDR ทั้งหมดได้รับการอัปเดตและสะท้อนถึงระบบ กระบวนการ และเทคโนโลยีปัจจุบัน แผนที่ล้าสมัยอาจทำให้ล้มเหลวเมื่อเกิดเหตุการณ์จริง

No Blind Spots (Dark Assets): ต้องไม่มีระบบสำคัญใด ๆ ที่อยู่นอกแผนการสำรองข้อมูล เช่น เซิร์ฟเวอร์ที่ฝ่ายการตลาดแอบตั้งขึ้นมาใช้เองโดยไอทีไม่รู้



No Ignorance of Employee Safety: ห้ามมีแผนที่เน้นการกู้ระบบ แต่ไม่มีแผนดูแลความปลอดภัยของพนักงาน ชีวิตคนต้องสำคัญกว่าเซิร์ฟเวอร์เสมอ

MIWCOM COMPANY LIMITED
32/41, 16th Floor, Sino-Thai Tower, Sukhumvit 21 Road (Asoke),
Khlong Toei Nuea Subdistrict, Watthana District, Bangkok 10110

“TREND KEYWORD 2026”

HAVE

MFA (Multi-Factor Authentication)

In the context of MFA, “HAVE” it refers to “Factors of Authentication” which is divided into three main categories:

Something you **KNOW**:
The information that only you can recognize
Example: Password, PIN, Security question.

Something you **HAVE**:
Physical or a Digital device
Example: Mobile phone (receiving SMS OTP), Token application (Google Authenticator), Smart Care or USB Key (YubiKey).

Something you **ARE**:
Information of Biometrics
Example: Fingerprint, facial recognition, Iris recognition.

MFA

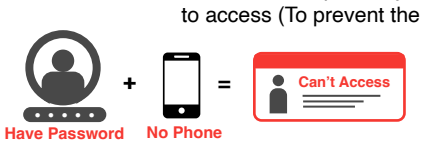
Access must be authenticated with a minimum of two factors.

Notifications are sent upon any login attempt.

DO NOT HAVE

In security context, “Do not HAVE”:
refer to the thing that must not occur to make MFA system strong.

No Single Point of Failure:
It must not have any vulnerability.
Example: If you only have a password and without mobile phone, you are not allowed to access (To prevent the password is leak).



No Static Access:
It must not have any “permanent access” without re-verification when changing devices or locations.

No Sharing:
OTP or fingerprint, it must not easily to share or transfer the others.

No Dependency on Password alone:
Do not solely rely on passwords, it is easily to intercept and guess.

NO VPN

The risks of SSL VPN or web VPN in 2024 – 2025, there was a highly critical issues in the cybersecurity due to Ransomware is a popularity vulnerability exploited and Hacker was attacked in a state-level.

RISKS IT HAS	Protections it does NOT HAVE
Risk of disguise with structure of SSL VPN:	SSL VPN cannot be prevented when compared with newer system of Zero Trust Network Architecture (ZTNA):
• **Have Critical Vulnerabilities**: In 2024 – 2025 was found vulnerability exploited RCE (Remote Code Execution) in popular device (e.g. Fortinet, SonicWall, Ivanti) that allow Hacker to control firewall without password.	• **No Continuous Verification**: Mostly of VPN that verifies just once when log-in at first. There is no re-verification while usage. If session was stolen, Hacker still use till it expire.
• **Have Implicit Trust**: Once the user gain VPN access, they often receive network-level access to the entire system. Occurring to allow hacker stolen the credentials and easily perform Lateral Movement.	• **No Device Health Check (in basic versions)**: SSL VPN often allow the device that “virus detected” or “not patched” to connect, making malware to spread from home network into office.
• **Have Browser-Based Risks**: Browser-Based (Clientless) that introduce the risk from malware embedded in browser such as Keystroke Loggers or Session Hijacking.	• **No Granular Application Visibility**: Administrators usually detected only “User A” is connected VPN but lack of the information that user is actually doing with application.
• **Have Public Exposure**: Logging in of SSL VPN portal, its exposure in public, making vulnerability scan or was attacked brute password force, 24 / 7.	• **No Protection against MFA Bypass**: If Hacker using a system of vulnerability exploited, they able to bypass to Multi-Factor Authentication check and directly admin.

Types of Risk	SSL VPN
Attack Surface	High (due to the web interface is easily visible to hackers).
Severity of Vulnerabilities	Frequent and intense (RCE vulnerabilities virtually every year).
Malware Protection	Low (especially when personal devices are connected).
Example	CVE-2024-21762 (9.8 of 10) CVE-2024-55591 (9.6 of 10)

SIRT

SIRT Security Incident Response Team (SIRT/CSIRT): This is about distinguishing between “readiness that must exist” and “failures that must be eliminated” to ensure effective handling of cyber crisis situations, as follows:

HAVE

A highly effective SIRT team must include four key components: People, Process, Technology, and Authority.

Have Clear Playbooks: There must be step-by-step procedures for each type of incident such as ransomware, phishing, and data leaks to reduce reliance on “instinct” and instead emphasize “standardized actions.”

Have Visibility: The team must have tools that provide clear visibility into what is happening within the systems, such as SIEM, EDR, and Log Management. If team “cannot see,” team “cannot fix the problem.”

Have Post-Incident Review: After every incident, there must be a “Lessons Learned” report to improve preventive measures and strengthen the system for future resilience.

DO NOT HAVE?

The obstacles or trap that a Security Incident Response Teams need to avoid to occur.

No Finger-Pointing Culture: During the incident, teams need to focus on “solving the issues” do not blaming individual. A blaming free culture ensure that the information is honestly and openly reported.

No Communication Silos: The information that must be contained smoothly between analysis team and manager. There is not any data that was kept and leads to make a wrong decision.

No Single Point of Failure: The system or process must be designed so that no single component failure can cause the entire system to stop functioning.

No Ad-hoc Responses: Do not respond or fix issues in an unstructured, short-term manner without having a long-term plan in place.

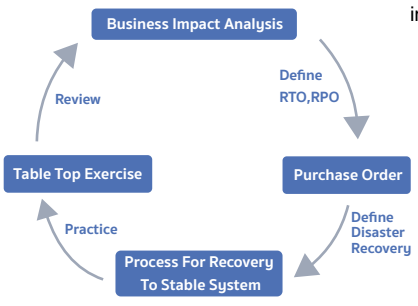
No Over-reliance on Tools: Expensive tools are useless if there is no one who knows how to interpret the data or perform in-depth analysis.

BCP

Developing a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP), collectively known as BCDR, is about preparing to ensure an organization can survive during a crisis. In summary, the difference between having (Have) and not having (Do not have) the BCDR concept is as follows:

HAVE

To cope with crises such as fire, flooding, or a ransomware attack, the BCDR team must include the following components:



Have BIA (Business Impact Analysis):
There must be an analysis to determine “If this part fails, how much financial loss will the organization incur?” This helps identify which areas should receive investment for protection first.

Have Clear RTO & RPO:
RTO (Recovery Time Objective):
It is crucial to set a clear timeframe for system recovery for example, specifying whether the system must be fully restored within a certain number of minutes or hours.
RPO (Recovery Point Objective):
Refers to the maximum acceptable amount of data loss measured in time. For example, if your RPO is 1 hours, it means the organization can tolerate losing up to 1 hours of data.

Have Tabletop Exercises (Plan Rehearsal):
A plan that is never tested is just a blank piece of paper. There must be scenario simulations and practical drills at least 1–2 times per year.

Have Offsite Backups (3-2-1 Rule):
There must be three copies of the data, stored on two different types of media and one copy kept offsite from office or in the cloud.

DO NOT HAVE

Common Failure Points That Cause BCDR Plans to Fail in Real Situations:

No Theoretical Plans: Avoid plans that look good on paper but cannot be executed in reality. For example, a plan that says “move operations to Building B” when Building B has no internet connection prepared.

No Single Person Dependency: Knowledge about system recovery must not reside with only one individual. If that person resigns or cannot be reached during an incident, the organization must still be able to restore systems using a documented playbook.

No Obsolete Documents: Ensure that all BCDR documentation is up-to-date and reflects current systems, processes, and technologies. Outdated plans can lead to failure during real incidents.

No Blind Spots (Dark Assets): There must be no critical systems excluded from the backup plan for example, a server secretly set up by the marketing team without IT’s knowledge.

No Ignorance of Employee Safety: Never have a plan that focuses only on system recovery without addressing employee safety. “Human lives must always be more important than servers.”

ZERO TRUST

If Have and Do not have, the ZTA system differs as follows:

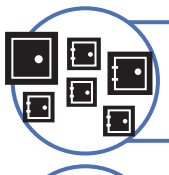
HAVE

To achieve the principle of “Never Trust, Always Verify”, a system must include the following components:

Continuous Verification: Involves ongoing checks, not just a single verification at login. It requires validating authorization and security throughout the entire session (on a per-session basis).

Strong Identity: Refers to having a clear and verified identity. It requires MFA (Multi-Factor Authentication) and additional context checks such as location, time of access, and user behavior.

Device Health Check: Involves verifying the health of a device before granting access to data. It ensures that the device is updated with the latest patches and checks whether antivirus software is installed.

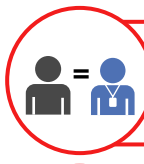


Micro-segmentation: Involves dividing the network into smaller zones, like having multiple small vaults, to prevent hackers who breach one point from moving laterally to other areas (Lateral Movement).

Least Privilege: Grant only the necessary permissions so employees can access only relevant information (Just-in-time & Just-enough access).

DO NOT HAVE

Zero Trust is designed to eliminate implicit trust and traditional vulnerabilities. Therefore, the following will not exist in this system:

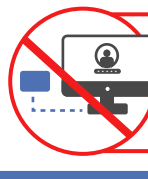


No Implicit Trust: Users must not assume that familiar individuals are safer or more trustworthy than unfamiliar ones. The system treats everyone equally and applies the same security measures to all.

No Trusted Perimeter: The network perimeter is no longer considered inherently secure. Every access request, whether from inside or outside the organization, must be verified and authenticated.

No Permanent Access: Users and devices are never granted indefinite access. Permissions are temporary, based on necessity (Just-in-time access), and revoked when no longer required to minimize security risks.

No Visibility Gaps: The system must maintain complete and continuous visibility across all activities, endpoints, and network segments. There should be no blind spots where malicious actions could go undetected.



No Reliance on IP Address: The system does not depend on IP addresses as a trust factor. IP can be spoofed or compromised, so identity and security must be verified through stronger methods such as MFA, device health checks, and behavioral analysis.

MIWCOM COMPANY LIMITED
32/41, 16th Floor, Sino-Thai Tower, Sukhumvit 21 Road (Asoke),
Khlong Toei Nuea Subdistrict, Watthana District, Bangkok 10110