CYBER SECURITY & DATA PROTECTION

Target and Performance

Long term target by 2030:

The company achieves international standards for cybersecurity and data privacy certifications.

2024 Performance: Achieved the 2030 target, with the company receiving NIST assessment scores for the 3rd consecutive year. The Company's average score is **4.22** (while National average score is 1.91)

100% Complied with Charoen Pokphand Group and external party action list for cybersecurity and data privacy.

- Total number of information security breach case = **0** case
- Total number of clients, customers and employees affected by the cybersecurity and data privacy breaches = **0** person
- Total number of clients, customers and employees affected by the data privacy breaches = **0** case
- **100%** of employees have been trained in cybersecurity awareness and phishing E-mail.
- **100%** of data routes have been conducted the cybersecurity risk assessment.
- **100%** of web and mobile application have been conducted the security testing service.

Cybersecurity Policy Structure

The Company has updated its cyber security policy, and cover more cybersecurity practices.

Cyber Security Management

Cyber Security Risk Assessment

Cyber Security Risk Mitigation

Cyber Security Continuous Management

Cyber Security Awareness

2024 Result:

- **100%** of employee has trained and communicated the cybersecurity policies

Cybersecurity Risk Management

Presently, cyber threats and attacks are more complex and impact cybersecurity risk. The company thus conducts 5-dimensional risk assessments cover a wide range of data routes that could be used to access company data, from head office, mobile phone applications, websites, as well as store and business partners.

Risk Assessment Guidelines	Risk Assessment Scope
Connecting to public networks	Company's servers
Phishing and ransomware	Employees
Identity theft	System administrators and employees
Supply chain attack	Information technology third parties
Information leakage	Employees

Cybersecurity Awareness Training and Discipline

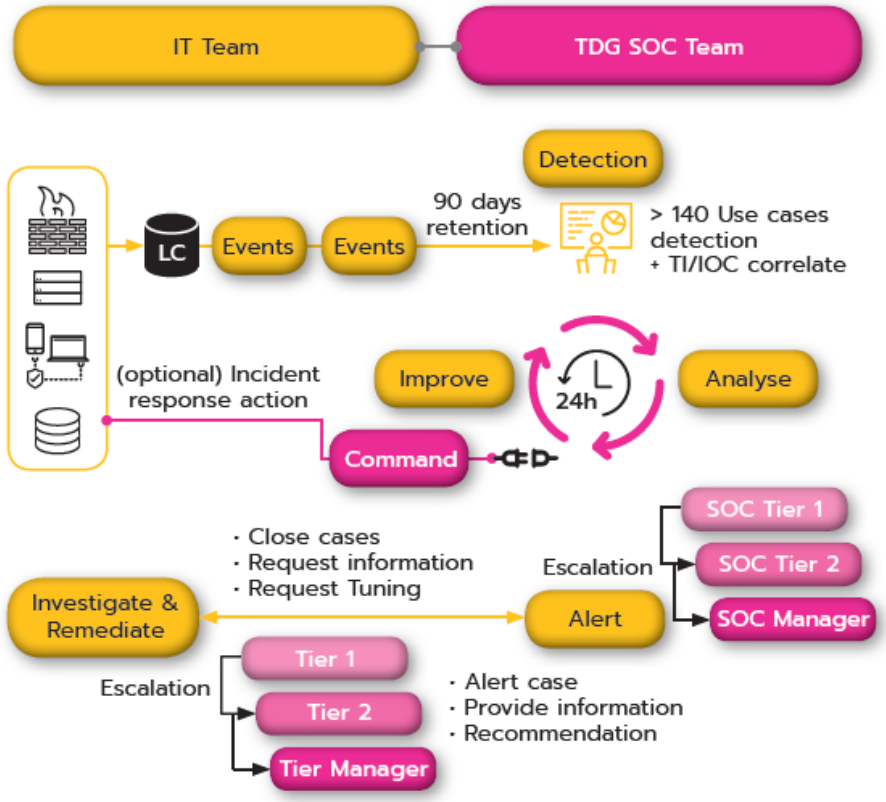
Awareness being the key to ensuring information system security against cyber threats and data leak prevention, approach is reinforced to raise corporate awareness; communication to introduce and create awareness, alerts to activate response awareness, and testing to assess cyber security awareness.

The cybersecurity is everyone's responsibility with being the one criteria of Annual Performance Evaluation and the year end bonus for employee both staff and manager levels must be reviewed the performance of discipline that related to cyber security and data protection policy.

Policy accessibility	• **100%** employees, can access relevant policy through the organization's internal communications website.
Communication	• **100%** employee are trained and communicated the Policies, information, and practices through training, internal communication email, and bulletin.
Response Instruction	• **100%** alerts that alarm relevant parties to internet leakage, security breaches, or susceptible emails.
Testing	• Identity theft phishing simulation (Phishing Test) to test employee awareness
Disciplinary	• **100%** employee must be reviewed the performance of discipline that related to cyber security and data protection policy and acknowledged prior computer login as below picture.

The Security Operation Center (SOC)“

The Company acknowledges the risks and has set up a 24-hour cyber security team to manage the Security Operation Center (SOC) with the objective of monitoring and responding to various threats in a timely manner under specified SLA and Charoen Pokphand Group information security standards.



Cybersecurity Awareness Training

The Company has organized training of the cybersecurity policy, awareness of suspicious and proper responding instruction to all employees as annually basis. The training course provides techniques to notice the 4 key scam patterns which are:

1) Emotive content
2) Invalid links
3) Invalid sender email addresses
4) Invalid email attachments

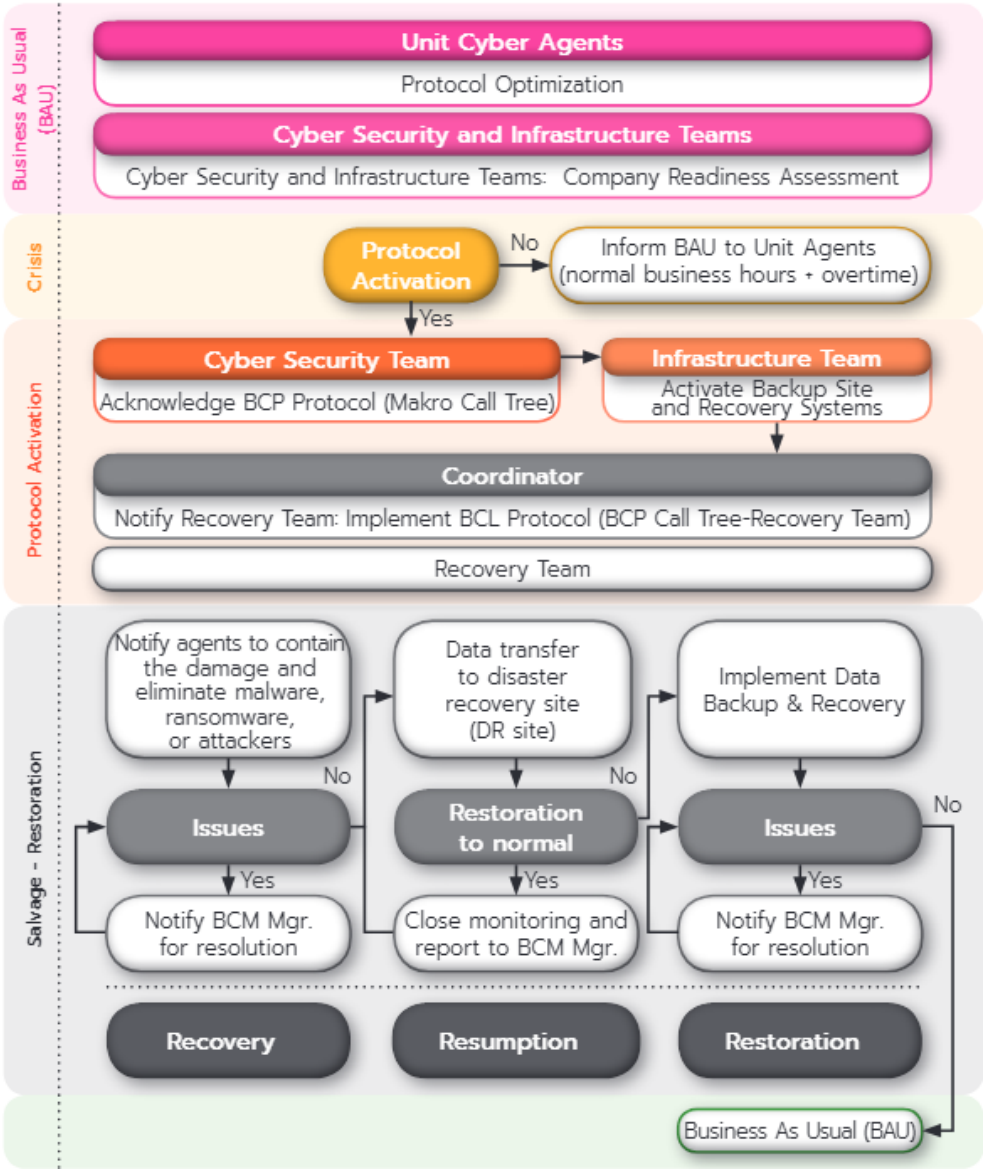
Including the instruction to response whenever they notice suspicious email or incident.

2024 Result:

- **2,953** trained employees (**100%**)
- **2,110** employees participated in email scam tests.
- **73%** has properly responded and **4%** reporting suspicious email.

Cybersecurity Business Continuity Plan

Following the framework of the ISO22301 to prepare for various crises that may occur and impact key business operations and the Company's risk management protocols. In 2024, the BCP drills are conducted twice.



Verification and Vulnerability Analysis by External Party

The company has conducted the external audit & Vulnerability Analysis by external party as NIST and external auditor to verity effectiveness of cybersecurity management system, infrastructure, and process.

Infra-structure & management systems have been audited

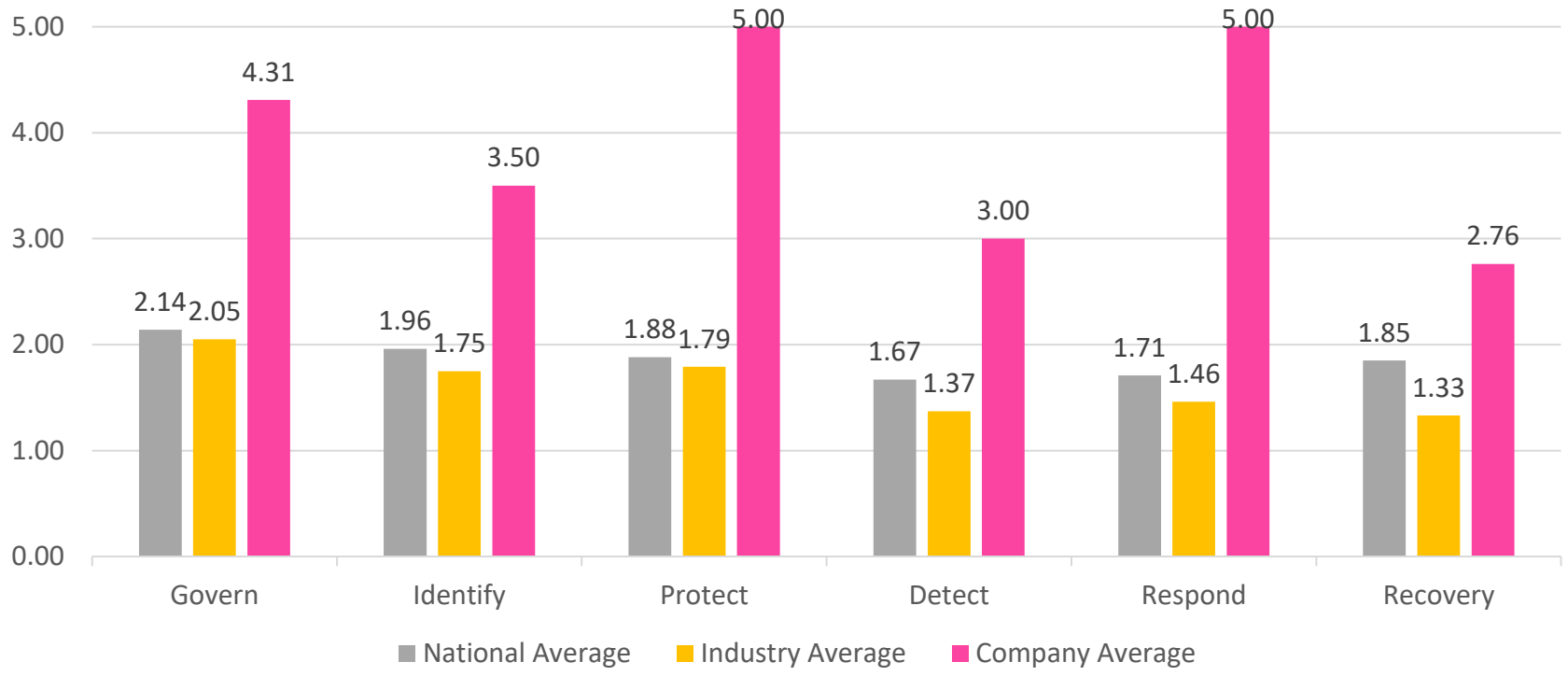
Vulnerability analysis by third party

Simulated hacker attacks by third party

Annual NIST Function Rating in 2024

The Company also participated the 2024 Cyber Security Assessment Program for Listed Companies under the Office of the Securities and Exchange Commission (SEC) and the NIST Cyber Security Framework that ranks organizational cyber security by readiness level. The program regularly verified the NIST Function's in 6 dimensions of Controlling system which are Govern, Identify, Protect, Detect, Respond, and Recovery for whole organization. The 2024 result shows the Company's score of **4.22** out of 5 levels which is highest rated comprising 202 of the companies that participated.

Score 4.22
Above NIST Function Average Rating



"Infrastructure Security Testing" (Hecker Attacks)

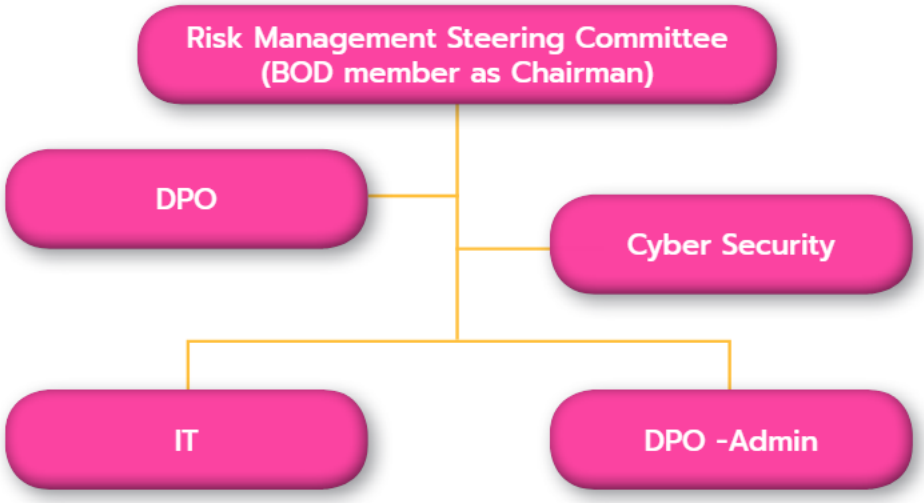
The Company hires the external party to simulate external hacker attacks (Red Teaming) to test the effectiveness of protection and evaluate the vulnerabilities in the system for improvement such as ASPX Debug Mode, Azure Domain Tenant, and Git-config Publicly Accessible.

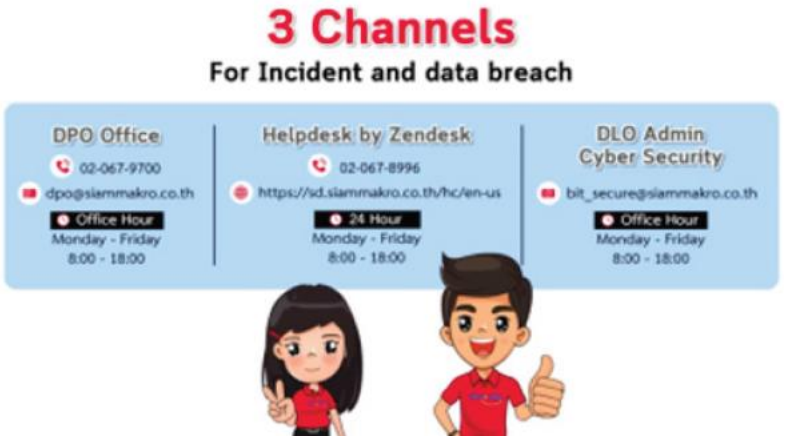
2024 Result:

- **100%** passed the security system test on all topics.
- No incidents of damage from cyber-attacks.

Data Privacy Governance

The Data Protection Officer (DPO) and department are designated responsible for privacy issues responsibilities to supervise the collection, usage, and disclosure of personal data, as well as conduct annual risk assessments, summarize the results, and report to the Risk Management Committee. The officer is also responsible for advising the committee and communicating with the entire organization on best practices and relevant disciplinary action, along with remedial measures for those affected.





Privacy Policy (PDPA)

The company Information Security Policy was announced to manage information security, confidentiality, availability, accuracy, and completeness of information compliance which applies to all entire operation throughout the business value chain, be it information of customers, supplier, contractor, and employee.

Data Privacy Policies & Procedures – Applies to all entire Operation, Supplier and Contractor

Data protection management

Data Protection Officer announcement

Training

Data Protection Risk Assessment

Customer Privacy Policy

Supplier Privacy Policy

Investor Privacy Policy

Employee Privacy Policy

Consent preference

Remedial action for breach case

Cookie Policy

Privacy policy for CCTV

The Company also implements measures to prevent breach case from unauthorized parties from access to personal information. Including prioritizes Personal Identifiable Information (PII) Security under Personal Data Protection Act (PDPA) and has announced a Data Protection Policies, as well as the installation of data management tools, namely the classification and labelling for data confidentiality and data loss prevention to automatically mitigate data leakage.

Scope and Implementation	2024 Result
Embedded in group-wide risk / compliance management	• **80%** of data privacy risk has reviewed and identified the mitigate plan
Disciplinary actions in case of breach	• **100%** employee must be reviewed as discipline that related privacy policy breach case during the annual performance and end year bonus evaluation. • **100%** employees, supplier and contractor are communicated partners, and contractors incidents of personal data leakage.
Third-party audits of the privacy policy compliance.	• On the process
Internal audits of the privacy policy compliance.	• **100%** were audited under annual internal audit compliance.

Customer Privacy Information

To protect customer's personal information from being leaked to outsiders or handled without proper authorization, and reduce the risk of data leakage and maintain data integrity and efficiency via a systemic approach and proper authorization which the information and instruction are issued. The External Privacy covers the following topics.

- Methods of collection and collected personal information
- Purposes of collection, use or disclosure of personal information
- Disclosure of personal information
- Sending or transfer of personal information to overseas
- Retention period of personal information
- Customer's rights
- Updating personal information
- Security measures of personal information
- Marketing information
- Coolies program and technical information
- Redirecting to other parties' websites
- Changes to the Privacy Policy
- Contact channel

2024 Result:

- **100%** employees trained Data Loss Prevention and Privacy Policies.
- **Zero** Customer, employee, supplier and contractor are impacted by data leakage or privacy breach case