Cyber Security Study - Questionnaire

Greetings,

This questionnaire is designed to study cyber-security practices and readiness in financial organizations In Nepal. The outcome of this survey will be presented in after FINTECH SUMMIT 2019 Nepal. The questionnaire is designed to maintain anonymity of the responder. Please provide your answers as realistic as possible.

Q. 1. Have you suffered any cyber-security breach in the last 12 months?

[ ] Malware [ ] Hacker attacks [ ] Virus attacks

[ ] Ransomware attack [ ] Weaknesses found during penetration testing

[ ] Lost assets [ ] Others [ ] Information not available

Q. 2. Which industry your organisation belongs to?

[ ] Finance [ ] Service [ ] Manufacturing

[ ] Retail [ ] Telecom [ ] Technology

[ ] Transport [ ] Others

Q. 3. What is the size of IT department?

[ ] 1-2 [ ] 3-5 [ ] 6-10 [ ] 11-15 [ ]> 15

Q. 4. Does regular audit of the your organization also cover IT audit?

[ ] Yes [ ] No [ ] When an issue arises

Q. 5. Have there been any IT audit conducted under the influence of requirements of regulator, business partner, or donor agency?

[ ] Yes [ ] No [ ] When an issue arises

Q. 6. What security frameworks and/or standards your IT department has adopted?

[ ] ISO/IEC 27000 [ ] COBIT [ ] ITIL

[ ] CARTA [ ] Regulatory standards [ ] Parent organization standards

[ ] Others [ ] None

Q. 7. Which of the following policies/procedures are documented in your organization and in effect?

[ ] Information security policy [ ] Cyber incident response plans [ ] Business continuity plan

[ ]Information security strategy [ ] Work under progress [ ] None

Q. 8. Does your organization have a dedicated department for network security?

[ ] Yes [ ] Yes, integrated with IT [ ] No

Q. 9. To whom the information security status is reported to?

[ ] Chief Finance Officer [ ] Chief Information Officer [ ] Chief Executive Officer

[ ] Board of Directors [ ] Information Security Officer [ ] Others

[ ] Information not available

Q. 10 what has raised the awareness on information security attacks in your organization?

[ ] Trainings & workshops [ ] Publications [ ] Legal/regulatory requirements

[ ] Attacks on the organization's IT infrastructure [ ] Attacks on client organization

Q. 11 How do you keep informed of new forms of information security attacks and threats?

[ ] Social networks [ ] Vendors [ ] Publications

[ ] Consulting firms [ ] News websites [ ] Conferences

[ ] Mailing lists / newsletters [ ] Others

Q. 12 What maturity level do you consider your organization is at the moment?

[ ] Level 1 Basic; undocumented, dynamic change, ad hoc, uncontrolled and reactive, individual heroics

[ ]Level 2 - Repeatable: some processes are repeated, perhaps with reliable results, poor discipline process,

[ ]Level 3 - Fixed: a set of defined and documented standard processes, some degree of improvement over time.

[ ]Level 4 - Managed: benchmarking process, effective management control, adaptation without losing quality.

[ ]Level 5 - Optimised: focus is on continuous improvement and innovation.

Q. 13 What do you think will improve your organization's security levels?

[ ] IT steering committee [ ] Better employee awareness [ ] Increased IT security personnel

[ ] Larger budgets [ ] Advanced security technology [ ] Senior management commitment

[ ] Employee rewards [ ] Others

Q. 14 What do you consider to be your greatest security risk?

[ ] Uncontrolled portable devices [ ] Internet downloads [ ] Incorrect configuration

[ ] Malware [ ] Ransomware [ ] E-mail virus

[ ] Attack attempts [ ] Insider attacks [ ] Others

[ ] Information not available

Q. 15 Which security measures has your organization implemented?

[ ] Safety endpoints [ ] Event logs management [ ] Vulnerability management

[ ] Encryption [ ] Disaster recovery sites [ ] IDS/IPS

[ ] Anti-spam solutions [ ] Firewalls [ ] Antivirus

[ ] Others [ ] Information not available

Q. 16 What tools does your organization use to detect attacks?

[ ] Self-developed tools [ ] Open source tools [ ] Commercial products

[ ] Information not available

Q. 17 What measures do you usually take to mitigate attacks?

[ ] Destination-based remote-triggered blackholes [ ] Intrusion prevention systems

[ ] Source-based remote-triggered blackholes [ ] Firewalls

[ ] Access Control Lists / packet filters [ ] Others

[ ] Information not available

Q. 18 Does your organization provide employee training to raise information security awareness?

[ ] Yes, during general training [ ] As per regulatory requirements [ ] As per job role

[ ] No

Q. 19 In your opinion, how difficult is it to convince management to invest in security solutions?

[ ] Very difficult [ ] Somewhat difficult [ ] Easy [ ] Very easy

[ ] Information not available

Q. 20 What percentage of your IT- budget was spent on security last year?

[ ] 0-10% [ ] 11-30% [ ] 31-50% [ ] More than 50%

[ ] Information not available

Q. 21 How does your organization ensure an adequate and appropriate level of information security over third parties such as vendors, business partners etc. ?

[ ] Regularly monitors and reviews third party services

[ ]Addresses information security issues in a contract

[ ]Signs confidentiality and/or non-disclosure agreements

[ ]Imposes corporate security policy and controls on third parties

[ ]Where permitted, performs background verification checks on selected high-risk

[ ]Controls third-party access to systems and data

[ ] Identifies risks related to third parties as part of information risk assessments

[ ]Performs random spot checks of third-party sites

[ ]Requires independent attestation (e.g. ISAE3402, ISO27001:2005 certification)

[ ]Others . . . . . .

Q. 22 Does your organization share information on information security attacks with other parties?

[ ] To regulators & police [ ] To consultants [ ] To general public

[ ] No

Q. 23 How confident are you in information security practices of your third parties?

[ ] Not confident [ ] Somehow confident [ ] Confident [ ] Very confident

[ ] Not applicable

Q. 24 How do you highlight information security weaknesses, risks, and non-compliance in your organization?

[ ] Input from peers [ ] Penetration testing [ ] Internal audit

[ ] External audit [ ] Information risk analysis [ ] Formal risk analysis

[ ] Input from vendors [ ] Assessment by regulator [ ] Others

CSRI Nepal (Center For Cyber Security Research and Innovation Nepal) can clearly determine cyber security issues and turn out applicable solutions and justify those solutions during a approach that everybody will perceive.
Founder President / General Secetary / Treasurer
Chiranjibi Adhikari / Dilli Chaudhary / Milan Raj Nepali
Email: info@csrinepal.org / csrinepal.org@gmail.com
Cell: +977-9860664392

Cyber Security Partner: **One Cover Pvt. Ltd.**

Community Partner: **npCert (Information Security Response Team Nepal)**

College Partner: **Texas College of Management and IT**

Training Partner: **DIT Solution**

Technology Partner: **ICT Frame Magazine Pvt. Ltd**

Software Partner: **Biz Sagar Pvt. Ltd.**

Prepared By: **Dr. Pramod Parajuli (Board Member at CSRI Nepal)**