# The Importance of Cyber Security Within Your Organization

BY TED BROWN

**You know that Cyber Security is an important Business Continuity Planning (BCP)/COOP issue, but like everything else in the BCP/COOP world, unless you get buy-in across the board, Cyber Security policies and procedures will be ignored.**

So the purpose of this article is to prepare you to articulate the importance of Cyber Security, to gain allies to implement procedures, and to justify the value of a Cyber Security Audit. After all, Cyber Security concerns more than the Information Technology (IT) and BCP/COOP departments.

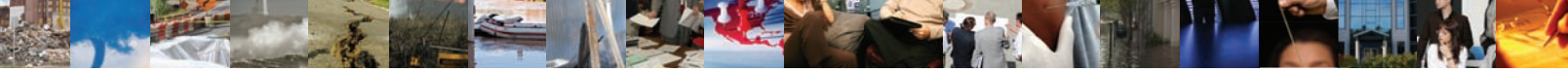
As the world becomes increasingly interconnected, Business Continuity/COOP professionals must pay more attention to the security of their organization's connections. It seems like every week there are new headlines about hackers bringing an organization to its knees. The stolen funds, bad publicity, and embarrassing revelations are front page news. How can you protect your organization from these issues? The best protection is to implement plans and procedures. And the best way to demonstrate the needs for those procedures is to perform a Cyber Security audit and implement the resulting recommendations.


## Cyber Security Audit

A Cyber Security audit can be performed internally, but it is almost impossible to effectively audit yourself. Sending a clear Request For Proposal (RFP) to potential audit suppliers will move the process forward quickly.

An outside cyber security audit RFP should cover the following areas:

- Your organization – your IT infrastructure, basic organization details, etc.
- The RFP process – selection criteria, timeline, submission guidelines, supplier qualifications (especially independent certifications)



- Scope
  - An independent external scan and vulnerability assessment (penetration testing) at the beginning of the engagement
  - Additional external scan and vulnerability assessment after remediation
  - Inventory of Devices – both authorized and unauthorized. Organizations have numerous servers, routers, switches, wireless devices, modems, firewalls and other devices that can be utilized by hackers. First you need to know what you have, then you need to update all systems to best practices, and finally you need to ensure best practices are performed into the future.
  - Inventory of Software – both authorized and unauthorized. Software concerns are similar to device concerns.
  - Verification of best practices for secure configurations of laptops, workstations, and mobile devices.
  - Internal security software assessment– you have purchased anti-virus, anti-malware, and other software for protection. Are they functioning correctly?
  - Assess if your current data backup and recovery policies allow you to recover from a major breech
  - Assess administrative privilege controls
  - Assess your incident response capability
- Deliverables – type of reports, discussions, training, remediation details, etc.
- Standard Terms and Conditions – including non-disclosure

Work with your IT department to ensure that implementing the resulting recommendations will make your organization more secure. Like most criminals, hackers look for easy targets. If your organization has easy to exploit security issues, hackers will dive right in. If your organization implements the resulting recommendations, hackers will become frustrated and move on to the next easy mark.

A subset of a Cyber Security audit is a Payment Card Industry (PCI) audit. PCI audits are required for organizations that process credit card transactions. A Cyber Security audit does not replace a PCI audit and a PCI audit does not replace a Cyber Security audit. Failing a PCI audit can result in revocation of your merchant account and/or fines starting at $5,000 a month. Worst case is a data breech with fines starting at $182 per data record. If you process credit card transactions, you need both a Cyber Security audit and a PCI audit.

## Developing Cyber Security Plans and Procedures Allies

Educate the decision makers – the lack of Cyber Security often has serious consequences.

A new report from the Privacy Rights Clearinghouse (PRC) notes 535 breaches during 2011, involving 30.4 million sensitive records. But that's a conservative estimate, since not all data breaches see the light of day. "Because many states do not require companies to report data breaches to a central clearinghouse, data breaches occur that we never hear about," said PRC director Beth Givens.

In addition to theft of organization funds, data breeches have HIPAA, SOX, credit card, privacy, and public relations issues. A data breech can quickly add up to millions in regulatory fines. You will usually find that Cloud suppliers take no responsibility for data breeches. Even if regulated data is not disclosed, a large data breech usually results in large additional costs and loss of customers.

## Recruiting Allies

Other departments within the organization also have Cyber Security concerns. Below is a partial list of departments who may be interested in becoming allies on the Cyber Security issue:

- Information Technology – This department may see Cyber Security as only an IT issue. They may welcome the support of additional departments and would be willing to be the lead department during the implementation. You must engage with this department since they will be needed to implement many of the resulting recommendations.
- Finance – is one of the main beneficiaries of a Cyber Security audit. Engage them by talking about how a Cyber Security audit is insurance that protects the organization's assets and improves SOX compliance.
- Security – Not all breaches are about money or data. Sometimes breaches are about creating access to the organization's facilities or threatening employees.
- Legal and Compliance – Approach this department with SLA, contract, and other legal exposures and they should be willing to assist.
- Sales and Marketing – Discuss the public relations fiasco they will have to deal with during a data breach and they should come on board.
- Customer Service – Ask them what kind of call volume they would expect once a data breach became public knowledge. You need to have a reliable estimate and the question will open their eyes.
- Human Resources – HIPAA compliance and possible threats to employees may motivate HR to become an ally.

## Conclusion

A Cyber Security audit is a great investment and improves your BCP/COOP. It works best when you have the support of several internal departments, especially IT. The cost to perform a Cyber Security audit, at a single location organization, conducted by an outside firm, can be as low as several thousand dollars. But, it's of no value if IT and the rest of the organization won't implement the recommendations. We hope the techniques above will help your organization to have a better BCP/COOP and avoid a Cyber attack.


### ABOUT THE AUTHOR

Edward B. (Ted) Brown III, CBCP CBCV MBCI, President & CEO of KETCHConsulting is a member of the Contingency Planning Hall of Fame and a newly elected BCI USA Board Member. He is a frequent contributor to the Disaster Resource GUIDE and a speaker at major industry conferences. You can reach him at tedbrown@ketchconsulting.com, or (484) 919-2966.