CYBER SECURITY BEST PRACTICES

DO YOUR PART.
#BECYBERSMART

Third Party & Supply Chain Cyber Management

As technology evolves, services that are outsourced and hosted by third parties will increase, as this has proven to be a very effective way for financial institutions to do business and remain competitive. However, the reward in efficiencies come with risk – specifically, cyber risk. With the rise and sophistication of third party and supply chain cyber breaches, there is no better time than the present to revisit risk management controls.

There is one thing that financial institutions have adapted to over the years – to develop risk management programs expecting that the worst can and will eventually happen. For financial institutions, this means that your typical Vendor Management Program should be enhanced to include cyber management controls over third parties and supply chain vendors. How many institutions today can say that they are actively monitoring third parties and supply chain vendors?

Per the National Institute of Standards and Technology (NIST), below are questions that financial institutions should consider to determine how risky their third parties' and supply chain vendors' cybersecurity programs are:

- How does the vendor stay current on emerging vulnerabilities?
- Is the vendor's software/hardware design process documented, measured, and tested?
- How are system settings managed and tested for code quality, vulnerabilities, and backdoors?
- What levels of malware protection and detection are in place?
- Are physical security controls in place, documented, and tested?
- What access controls are in place to systems and data?
    - How do they protect and store customer data?
    - How is the data encrypted?
    - How long is data retained- while the contract is active and after contract termination?
    - How is the data destroyed once the relationship has ended?
- What type of employee background checks are conducted and how frequently?
- How does the vendor vet and monitor their third parties and supply chain relationships?
    - What process is in place to make sure security practices are being followed?
- Have all internal and external channels been clearly documented (i.e. network connection diagrams, data flow diagrams, etc.)?
- How does the vendor assure adherence to security principles and controls?

Buckley Technology Group is trusted by financial institutions nationwide to develop and deliver Vendor Management & Due Diligence Programs that meet evolving cyber risks and security best practices. Our outsourced Vendor Due Diligence professional services and ISSAC Online compliance software solutions ensure your institution is prepared and protected.

Need help creating an effective Vendor Management Program?

For more information, contact one of our certified Compliance Consultants at **(800) 355-4550** or visit **www.buckleytechgroup.com**

BTG
BUCKLEY TECHNOLOGY GROUP