4 Important Cybersecurity Focus Areas for Banks

Banks face an evolving set of threats from both internal and external sources. The sophistication of criminal and hacker methods continue to increase; exploiting vulnerabilities directly, or through connected third parties. Bank Cybersecurity Officers must face these and other security challenges, while at the same working across all parts of the bank to increase security awareness.

Northcross Group (NCG) helps Bank Cybersecurity Officers address these evolving security challenges with direct support, tools, and consultation. NCG's Team has a unique blend of banking experience at the regional and national levels; combined with cybersecurity expertise built in the defense, intelligence, and private sectors. The following are 4 key Bank cybersecurity focus areas that NCG supports Bank security teams and leaders.

#1 - Increasing Regulator Focus on Bank Cyber Risks…

Regional, Super-Regional, and National Banks are reviewing their current security programs and infrastructure in light of increasing scrutiny from the OCC.

United States Comptroller of the Currency Thomas Curry (a former chairman of the FFIEC) continues to highlight a focus on cybersecurity and its role in examinations. FFIEC is releasing its Cybersecurity Assessment Tool, which is modeled after the NIST Cybersecurity Framework. The OCC has cited the value of the tool for banks as part of their cybersecurity focus and measures. The scope of this focus draws lines outside of the Bank controlled networks to those of third parties based on OCC 2013-29 guidance.

Next Steps: NCG helps security and risk management teams assess their current security posture and program maturity in preparation for enhanced cyber considerations in future bank examinations. NCG brings a depth of experience having been part of the NIST working group that developed

the Cyber Security Framework, and has deep experience in banking. This unique combination of cybersecurity and banking expertise helps banks address cybersecurity objectives aligned with the overall strategic path of the Bank.

#2 - Implementing an Enterprise Cyber Risk Management Process…

Banks of all sizes are working to address gaps in, or a lack of, a true enterprise cyber risk management process—a key element of the FFIEC Cybersecurity Assessment Tool.

Risk management processes are often implemented with too much complexity or such levels of abstraction that they are not very useful. An effective enterprise risk management process can be invaluable to the Bank. The risk management program is also a key indicator of a Bank's cyber capability maturity.

Next Steps: NCG has helped Banks build successful and sustainable risk management programs that align with their current culture and capabilities. From that starting point, the process can be enhanced and improved while keeping the active engagement and participation of the organization.

#3 - Enhanced Incident Response Capabilities…

The technologies in place, and being actively deployed by Banks, are the very ones hackers and criminals are using with increasing effectiveness.

Internal and external threats continue to evolve in capability and complexity. Customers and employees represent a more mobile and interconnected set of access points—as well as a network or third parties—that require a robust and ready incident response capability. When something goes wrong, there needs to be a framework to manage your response and actions effectively across different stakeholders.

Next Steps: NCG works with Banks to bolster and support continuous improvement of capabilities across the incident response life cycle. From detection to response and recovery, we help Bank security teams develop and exercise response processes that cover direct and connected operations effectively.

NCG Bank Cybersecurity Services:

Connecting People, Data, Infrastructure & Processes

- Security Program Development & Enhancement
- Third Party Risk Assessments
- Security Project Management & Execution
- Security Consultation & Advisement

#4 - Budget, Process, and Resource Alignment between Security and Solution Development…

Banks have enjoyed success with better integration of security objectives with current Bank SDLC/PMLC processes and key strategic initiatives.

The engagement model for information security interfacing with solution architecture and delivery has changed. In some cases, however, project teams and day-to-day practices are typically operating under the old model where security is a checkpoint or reviewer; not part of the solution definition. If aligned properly, the projects driving change and progress can be geared to deliver security value as well.

Next Steps: NCG works with project management offices and information security teams to improve process for consideration and forecasting of security concerns across projects and systems. Our team works with Bank project teams to facilitate a proactive engagements and implement sustainable processes for the future.

The Northcross Group (NCG) delivers business system and technology services. NCG makes it our business to ensure that technology serves our clients, allowing them to meet business goals, gain competitive advantage, enhance security, implement governance, ensure compliance, and stabilize operations.

NCG consultants bring a blend of technical and business acumen with a proven track record in the public, private, and non-profit sectors. We approach business challenges head-on and figure out the most effective way to leverage technology to reach objectives.

NCG uses disciplined processes, refined from decades of experience. Flexibility is a cornerstone of our industry-tested methodologies—giving NCG the ability to adapt to changing environments and needs.

www.northcrossgroup.com
info@northcrossgroup.com

100 Middle Street, East Tower, #203
Portland, ME 04101
Phone 207.699.5540
Fax 207.699.2113

1101 Wilson Boulevard, 6th Floor
Arlington, VA 22209
Phone 703.351.3397
Fax 703.351.5298