

Merchant Capture Threats

Wednesday, February 2nd – 2 PM to 3 PM CST

Presented by Kevin Streff, Ph.D., Director of the National Center for the Protection of the Financial Infrastructure at Dakota State University

According to a recent report, the costs of having the checks lying around far outweigh the costs of remote deposit capture. Consequently, banks are widely adopting merchant capture solutions to both control expenses and increase customer service. This informational webinar will provide insight into the information security risks for merchant capture solutions and associated service providers. Threats will be identified for merchant capture systems in both a hosted and outsourced environment. Each threat will be discussed for probability and impact, so that participants can include it on their risk assessment. Mitigating countermeasures will be examined for each threat so that they too can be included on your risk assessment. After completing this seminar, attendees will gain an understanding of which threats pose serious risk in a merchant capture environment, and what you should do to mitigate this risk to an acceptable level. The webinar will answer the following questions:

1. What are the common merchant capture architectures?
2. What are the security threats for each of the common merchant capture architectures?
3. What is the probability of each threat to occur?
4. What is the impact if each threat occurs?
5. What are the mitigating countermeasures for each threat?

Space is limited. Reserve your Webinar seat now at <http://bit.ly/MCthreats>

Mobile Banking Threats

Wednesday, May 4th – 2 PM to 3 PM CST

Presented by Kevin Streff, Ph.D., Director of the National Center for the Protection of the Financial Infrastructure at Dakota State University

Mobile Banking is identified as the number one technology bankers are looking to deploy and scale over the next two years. However, information security threats to this environment are serious. This informational webinar will provide an inventory of mobile banking threats for three common mobile banking architectures: text-based, download and thin-client. Each threat will be discussed for probability and impact, so that you can include it on your risk assessment. Mitigating countermeasures will be examined for each threat so that they too can be included on your risk assessment. After completing this seminar, attendees will gain an understanding of which threats pose serious risk in a mobile banking environment, and what you should do to mitigate this risk to an acceptable level. The webinar will answer the following questions:

1. What are the common mobile banking architectures?
2. What are the security threats or each of the common mobile banking architectures?
3. What is the probability of each threat to occur?
4. What is the impact if each threat occurs?
5. What are the mitigating countermeasures for each threat?

Space is limited. Reserve your Webinar seat now at <http://bit.ly/MBthreats>

Information Security Program (ISP) for Small-and-Medium Financial Institutions

Wednesday, August 3rd – 2 PM to 3 PM CST

Presented by Kevin Streff, Ph.D., Director of the National Center for the Protection of the Financial Infrastructure at Dakota State University

Gramm-Leach-Bliley requires financial institutions to develop and implement a comprehensive, risk-based information security program to safeguard sensitive customer and financial information. The information security program is the basis for the I.T. examination conducted by state and federal regulators. However, most banks lack a top-down, management-driven information security program that fits their bank's unique needs, including the technologies they deploy and the risks they have. This informational webinar will provide an overview of what a good information security program looks like, what each of the components of the program are, and how each of the program components work together to safeguard your institution. The webinar will answer the following questions:

1. What should be included in an information security program for small and medium-sized banks?
2. How does risk assessment drive the content of the information security program for a small or medium-sized bank?
3. How does each of the components of an information security program fit together?
4. How can I get efficiency in managing my information security program?

5. What are some of the best practices I can include?

Space is limited. Reserve your Webinar seat now at <http://bit.ly/ISP-SMFIs>

Security Awareness Training Ideas

Wednesday, November 2nd – 2 PM to 3 PM CST

Presented by Kevin Streff, Ph.D., Director of the National Center for the Protection of the Financial Infrastructure at Dakota State University

People are often considered the number one security threat! Consequently, it is imperative that your bank develop and implement a comprehensive information security awareness program for employees, business partners and customers. However, the current state of security awareness with customers (through privacy policy mailers) and employees (through an annual security awareness presentation) simply falls short. This informational webinar will provide an inventory of affordable and creative security awareness ideas that are sure to add real value to your bank. The webinar will answer the following questions:

1. What creative / affordable ideas are there to promote security awareness with customers who are conducting Internet Banking or Mobile Banking?
2. What can my bank do to promote security awareness with business partners and commercial customers?
3. What creative / affordable ideas are there to promote security awareness with employees?
4. How do I use my risk assessment to drive my security awareness program?
5. Is there anything free I can use out there that will help with security awareness?

Space is limited. Reserve your Webinar seat now at <http://bit.ly/SecurityAwareness>