Addressing Insider Threats, Cyber Attacks & Data Security

Insiders

Community banks differentiate themselves by delivering high levels of customer service. The United States now has well over 6,000 community banks that hold trillions of dollars in assets. The simple cyber security math in this equation results in an extremely large and fragmented attack surface containing valuable personal and financial information that is aggressively pursued by nefarious groups and individuals.

These banks must evaluate their cyber security as they would any level of business risk. Risk-related business questions are commonplace: Should we open up a new branch? Should we embrace more online services? Should we invest in new technologies to better serve our customers? However, these business discussions must also consider cyber security risk questions such as: Are we protecting our customers from external attacks? Do we have the controls in place to mitigate malicious insiders? Do we even have the viability into our own systems to determine if we are secure, under attack or compromised?

Careless and malicious insiders are often the most difficult threat actors to manage. This is particularly true for smaller community banks that may not have the time, technical resources or human resources to mount an effective insider threat mitigation security program. Securonix can help by:

* Providing greater visibility into user interactions across critical systems
* Automatically baselining “normal” behaviors, and alerting on behavior outliers
* Allowing more rapid threat identification and incident response with reduced complexity and easy to understand incident workflows
* Operating as a central source for not just insider threat mitigation, but also external threat mitigation by correlating disparate logs and alerts from endpoints, network devices, data security solutions, physical security solutions and the like
* Reducing investigation time and resources

Perimeter

Perimeters are always evolving and prevention alone doesn’t scale. Simply trying to build the highest wall and dig the deepest moat is not an effective strategy. As General George S. Patton said, “Fixed fortifications are a monument to the stupidity of man.”

A defense in depth strategy can be valuable where preventative controls are augmented by incident detection and incident response. However, if these solutions exist in a silo and are not integrated through a centralized security analytics platform that correlates events from preventative and incident detection controls and, most critically, incorporates incident response, you’re left with a slow, outdated security posture without contextual relevance. In short, you get too many alerts and not enough results.

The number one enemy of security is complexity, and the best weapon to fight complexity is context. A security analytics platform that unlocks the actionable context from your existing infrastructure to find the causal relationships between, people, network activity, data, time, etc., is what community banks need to stay efficient and effective in the fight against security threats.

Data

Community banks, just like every financial institution, generate massive amounts of data noise. It’s akin to looking at a TV channel that is mostly static, only occasionally being able to make out a person or place.

Having a data security solution like DLP with the contextual relevance afforded by a security analytics platform reduces that noise. In fact, many financial institutions have found that the volume, velocity and variety of data that DLP processes yield far too many alerts. Without human context and other sources of relevance, having a data security solution can result in rapid resource drain.

Securonix isn’t focused on insider threats or perimeter threats or even data alone. Rather, Securonix works across all three of these disciplines and incorporates other critical variables to reduce complexity, increase context, reduce remediation efforts, save time, save money and allow banks to focus resources on servicing customers. Securonix detects threats automatically and accurately so that banks don’t have to becoming experts in insider threat mitigation, breach response and data security.

Chris Inglis
Chairman of the Securonix Strategic Advisory Board

SECURONIX
Security Analytics. Delivered.

Contact Info

www.securonix.com
(415) 241-9000

Chris Inglis is Chairman of the Securonix Strategic Advisory Board. Securonix is a company that has developed purpose-built advanced security analytics technology that is able to detect the most advanced data security, insider threats and fraud attacks automatically and accurately. Mr. Inglis is former deputy director at the NSA. He attended the United States Air Force Academy, graduating in 1976 as a Distinguished Graduate with a Bachelor of Science Degree in Engineering Mechanics. He holds numerous prestigious Medals and Awards including the President's National Security Medal, Director of National Intelligence Distinguished Service Medal, Presidential Rank Award for Distinguished Service, U.S. Air Force Distinguished Service Medal, Presidential Rank Award for Distinguished Service, Deputy Director of Operations Special Recognition Award, and many more.