



## Partnering With Credit Unions to Address Data Security Challenges



### Compliance Issues

#### Why is data security becoming so critical in the credit union industry?

- Data, or “information”, is one of a credit union’s most important assets.
- Timeliness and reliability of data is vital.
- Protection of data is critical in establishing and maintaining trust between the CU and its members.
- With the recent compromised plastic cards events as well as rising incidents of identity theft, regulators are now focusing on data security and monitoring controls heavily. An Intrusion Detection System is an intricate part of any adequate Information Security Program.

#### What is an Intrusion Detection System (IDS)?

- A solution that inspects all inbound & outbound network activity and identifies suspicious patterns that may indicate an attack from someone attempting to break into or compromise a system.

#### Why is it so important that credit unions implement an IDS?

- The FFIEC implemented section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLBA) by clearly defining a process-based approach to financial institution security in their “Interagency Guidelines Establishing Information Security Standards” document.
- These GLBA 501 (b) guidelines outline enforcement options granted to the FRB, FDIC, NCUA, OCC, and OTS in the event that financial institutions do not establish and maintain adequate information security programs.
- The critical nature of data security, as well as responsibilities and monitoring requirements are very clearly defined – including the need to collect and store device logs, implement network and host traffic policies, and adequately monitor activity to detect and act on potential attacks.

#### What challenges do CU’s face as they implement an IDS solution?

- Every network includes many devices and components. These devices and operating systems produce logs that the IDS uses to collect and analyze data to identify potential intrusion attempts.
- The high volume as well as complexity of monitoring events requires an in-depth level of understanding of the data being collected – real time monitoring is highly recommended.
- The magnitude of the volume of events generated (millions per day, in some cases) can create the need to hire a FT resource (at a very high cost) to stay on top of potential threats/attacks.

#### What is CRI Solutions’ answer to address these challenges?

- iSec® (Infrastructure Security Monitoring)