2 days has 48 hours or 78 crores?

"In two days, hackers withdrew a total Rs.78 crore from various ATMs in 28 countries, including Canada, Hong Kong and a few ATMs in India, and another Rs.2.5 crore were taken out within India," Cosmos Bank chairman Milind Kale. A well-known planned robbery where dummy cards were made for cash withdrawals causing 12000 transactions across 21 countries. A typical case of intentional negligence and definite plan of robbery. With limited resources (time, staff, and budget), setting up an operations center supported by multiple monitoring technologies and real-time threat updates doesn't seem all that Do it yourself. That is where the security organizations come into picture.

Online security is a vital concern for banking online marketplaces, with money contained within digital wallets that have increasingly become a target for hackers as the number of currency stored and their value has skyrocketed over the last years. A popular target for hackers since the trail goes cold easily and cybersecurity criminals can digitally erase their footprint. There is a continued vulnerability and a need for cyber security .With advancements in technology, hackers are becoming more skilled at finding holes and cracks in corporate security systems and can gain access to protected files and data, posing a significant cybersecurity threat-Corporate security breaches, hacktivism, leakage through botnets, spear phishing, social media security breaches etc.

There is a price to pay when a half-hearted security plan is put into action. It can result in unexpected disaster. Startups, banks, other financial institutions are more vulnerable to attacks mainly because of the weaker security as they may not have enough computers and servers on the network to verify transactions. Such platforms with lesser processing power become easy targets for hackers with superior processing power. Fortunately, as technology has advanced, so has the ability to seek out cybercrimes before they happen and protect people when they occur.

Organizations will need to determine the price they are willing to pay in order to protect data and other assets:

- Protect networks and data from unauthorized access.
- Improved information security and business continuity management
- Improved stakeholder confidence in your information security arrangements
- Improved company credentials with the correct security controls.
- Faster recovery times.

Improving the cyber security of banks and credit unions continues to challenge many IT organizations. Regional banks and credit unions in particular often lack the resources to keep up with the increased sophistication of the threats targeting their networks. These smaller financial services organizations don't have the budget to hire dedicated security practitioners or invest in the diverse security controls needed to detect and respond to threats quickly. They also lack the ability to respond quickly to changes in the regulatory environment. One needs a full proof solution for cyber threat detection, threat prioritization, integrated threat intelligence. Cybersecurity organizations have a continuous monitoring of your network, users, and assets, identify suspicious and malicious activity quickly helping you to Correlate and analyze security events from built-in data sources and legacy tools.