# RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type: Awareness | Watch | **Warning**

## Recent Ransomware Attack Validates Growing Trend Targeting Vendors

A major provider of automatic teller machines (ATMs) and payment technology, Diebold Nexdorf, recently suffered a ransomware attack that disrupted some corporate operations and services for over 100 of the company's customers. While Diebold has determined that the spread of the malware has been contained, the attack validates a growing trend of third-party vendors being aggressively targeted by cybercriminals deploying ransomware in 2019, according to Beazley Breach Solutions.

### Details

According to Diebold Nexdorf, the company's security team discovered anomalous behavior on its corporate network in April. Suspecting a ransomware attack, it immediately began disconnecting systems on that network to contain the spread of the malware. Diebold's response affected services for over 100 of their customers.

Diebold reports that the hackers never touched its ATMs, and that the intrusion only affected its corporate network and did not affect customer networks or the general public.

Cybercriminals have realized that interrupting the dependent and deeply interconnected relationship between vendor and customer would create the most pressure. It is believed that criminals attack these organizations where the odds of receiving a ransom payment is greater due to the potential business impact.

Third-party vendors were aggressively targeted by cybercriminals deploying ransomware in 2019, and at least **17% of all ransomware incidents** reported to Beazley originated from attacks on vendors. These attacks caused business interruption to many downstream customers, ranging from the inability to access data housed in a software application, to a full blown attack on the customer systems.

Ransomware can be devastating to an individual or an organization. Traditionally, these attacks were designed to deny access and interrupt business operations. However, the recent shift towards ransomware paired with banking trojans, and threats to expose data, changes the landscape.

The most common forms of attack used to deploy ransomware:

- Phishing emails with malware and links to credential-stealing websites or apps; and
- poorly secured remote desktop protocol (RDP)

**Date:** May 19, 2020

**Risk Category:** Ransomware; Fraud; Cybersecurity; Malware; Breach

**States:** All

**Share with:**

- ☐ Board of Directors
- ☐ Executive Management
- ☐ IT
- ☐ Risk Manager
- ☐ Vendor Relations

Your feedback matters!

**Was this RISK Alert helpful?**

Vote Yes | Vote No

# Recent Ransomware Attack Validates Growing Trend Targeting Vendors

**TYPICAL RANSOMWARE SCENARIO**

**Initial compromise of your environment**

- Fraudster targets your organization with a phishing campaign or through a poorly secured remote desktop protocol (RDP).
- Malware is successfully delivered to one of your unsuspecting users via a malicious attachment or web link in an email.

**Malware is downloaded and installed**

- The user opens attachment and malware is unknowingly installed on the user's PC.
- The hackers undetectably explore your network looking for vulnerable systems and sensitive data.

**Ransomware is deployed**

- With access achieved, ransomware is spread across your network encrypting indiscriminately.
- Attackers have now encrypted and disrupted a material portion of your business.

**Extortion**

- The attackers demand a ransom – up to millions of dollars – for the decryption key.
- The attack can also become public knowledge which causes reputational damage.
- The regulator also wants to understand if there has been a mishandling of customer sensitive data.

## Risk Mitigation Tips

Credit unions should consider these loss controls to minimize ransomware attacks.

- Lock down RDP.
- Require multi-factor authentication (MFA).
- Disable PowerShell on workstations where possible.
- Patch systems and internet browsers. Stay on top of anti-virus software updates to detect new emerging threats.
- Apply web filtering at the network and endpoint level that blocks connections to known-malicious sites.
- Limit administrative rights.
- Conduct security awareness training for employees on how to recognize common threats and scams and how to report any suspicious security incident.

## Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk resources to assist with your loss control. The Protection Resource Center requires a User ID and password.

- Partner Perspective on Ransomware: Beazley's 2020 Breach Briefing
- Cybersecurity Threat Outlook eBook
- Ransomware Prevention & Response Checklist

**Access the Protection Resource Center for exclusive resources:**

- Loss Prevention Library for resources & checklists
- Webinars and Education
- RISK Alerts Library
- Report a RISK Alert

The Protection Resource Center requires a User ID and Password.

**Facing risk challenges?**

Schedule a free personalized discussion with a Risk Consultant to learn more about managing risk.