Acumatica
The Cloud ERP

Cyber Incidents: Prevention and Proactive Response

CONTENTS

Acumatica Security Team

Introduction

This document outlines steps Acumatica takes to prevent or respond to incidents, including developing a cyber incident response plan. It also addresses the Acumatica Cyber Security Team ("Security Team") role in preventing and containing incidents as well as customer notification and communication with law enforcement.

Cyber-incidents, including hacking business websites and computer systems, are increasingly common. These incidents can be extremely damaging to businesses and other organizations, particularly if security is breached and confidential business and personal data compromised. Cyber-incidents and the resulting security breaches are part of a rapidly expanding international cyber threat that costs companies and taxpayers billions of dollars each year in lost information and response costs. Executives face increasing pressure to prevent these incidents and must act immediately to contain any damage once an incident occurs.

Here are some of the key areas of focus provided in this document:

- The Acumatica Security Team's key role in preventing and containing cyber-incidents.
- Proactively developing a cyber incident response plan to report, investigate, and respond to a cyber-incident.
- Acumatica Cyber-Incident Response Plan.

Cyber-incidents involving customer data implicate various data privacy and security laws. Acumatica is continuously working to improve our data security posture for our customers and the company.

Actions Acumatica Take to Prevent or Reduce the Risk of Cyber-Incidents

There are several resources the Acumatica Security team utilizes in developing a plan to prioritize preventative actions, for example, the National Institute of Standards and Technology (NIST) Framework Cyber Security Framework (CSF) for Improving our overall Cybersecurity posture. The Framework is a voluntary risk-based set of best practices and industry standards developed to enhance security and resilience in cyber. Generally, however, the focus is on process and technologies, but Acumatica strives to put more emphasis on education and security awareness for its employees on a quarterly basis.

Enhancing Cyber Security Layers

Acumatica continues to invest in enhancing our data security controls and procedures to deter or prevent cyber-incidents. These include the most up-to-date IT protection measures, for example:

- Maintaining a current asset inventory for all computer and network hardware and software.
- Using secure configurations.
- Monitoring vulnerability reports and applying the latest security patches.
- Granting access only to those with a demonstrated business need to know.
- Protecting all passwords.
- Using read-only views of documents and materials when possible.
- Encrypting important or sensitive data and personal information.
- Using current anti-virus software and other measures to protect against malware.

- Building security into applications and systems using security-by design principles.
- Testing mobile apps, websites, and devices to identify and address potential privacy issues and security lapses.

Acumatica has developed, implemented, and maintains sound network security architecture and controls, such as:

- Network segmentation.
- Next-gen Firewalls with intrusion detection and prevention services.
- Monitoring and managing log files to detect security incidents.
- Monitoring activities and procedures of third parties with access to the company's
- network and computer systems, whether direct or remote.
- Performing network scans to assess vulnerabilities.
- Continuous monitoring of activity on the network.

Acumatica's DevSecOps program is continuously improving. Below are some of the measures taken as part of the security enhancement for the program.

We address common web application security issues by:

- Creating names for tables and fields that are difficult to guess.
- Housing databases, applications, and web services on separate servers.
- Maintaining strict input validation.

Data Security

Acumatica ERP handles data security and compliance very diligently. Some of the data security functionalities include role-based access controls, database restrictions and limited administrative access, among numerous other features to ensure data security for our customers.

Portal Access

Acumatica ERP data security is compliant with many industry standards. For each customer, accessing their login portal directly will be done with a 256-bit TLS encrypted session connection. We provide options to utilize multi-factor solutions of the customer's choice either in the form of single-Sign-On or identity authenticator applications.

Sophisticated Database Restrictions

Data transmission across the systems utilizes our custom attribute encryption as well as token-based application authentications, such as identification, in order for data to be encoded with industry-standard encryption protocol.

Acumatica ERP database security implemented is a three-tiered level between user data and the Cloud application. The digital infrastructure is so powerful that only designated users can have access. Acumatica ERP has the ability to block access to its databases. In other words, there is no direct access to the main database, only the application.

Role-Based Access (RBAC) and Idle Disconnect

Acumatica ERP provides customers with the ability to provide role-based access that is directly related to their professional responsibilities and the data available to them is compliant with their job role.

Additionally, we provide the ability for custom session time-outs. While there is a limit for the max amount of time for a session time-out, we provide flexibility for those who are utilizing Acumatica ERP while working with or in other documents or systems.

The ability to audit all activity within the Acumatica ERP solution is key. For this we provide reporting for the date, time, location, and login details of users are documented on every entry and exit of the platform. You will know instantly if there's an intruder or if someone has logged in somewhere unexpected.

Password Policy and Protection

Acumatica asks that it's customer's creative in their password selections as our system prohibits the use of previous passwords. Acumatica ERP access security also has a minimum password length and requires all Acumatica ERP customers to regularly update their passwords.

Acumatica ERP's password policy requires each user's password to have numbers, letters, and special characters. Be considerate while choosing combinations for your passwords. There is an automatic lock out for multiple unsuccessful logins.

Acumatica's Digital Security Supply Chain

The Security Team continuously evaluates the Company's entire digital security Supply chain. If even a single link is weak, the Company could be vulnerable to incident. The Security Team is cognizant of interdependence and maintains status by providing the following as required for company stakeholders:

- Map the existing digital security supply chain.
- Identify and address key challenges to the digital security supply chain, including potential security risks.
- Encourage digital security supply chain engagement.

Acumatica's Cyber Incident Response Plan

Acumatica has developed a written plan (cyber incident response plan) that identifies cyber-incident scenarios and sets out appropriate responses. The cyber incident response plan also includes our global response plan. The Incident response plan's framework is based on these basic components:

- Response team
- Reporting
- Initial response
- Investigation
- Recovery and follow-up
- Public relations
- Law enforcement

Discovery and Reporting of Cyber Incidents

The cyber incident response plan outlines procedures for discovery and reporting of cyber-incident incidents from our designated Security Operation Center (SOC) These would include but not limited to:

- Monitor Acumatica's information systems are appropriately updated and secured.
- Continuously monitoring the Company's computer and network logs to discover any incidents.
- Creating incident tickets to track all reported incidents.
- Creating a risk rating to classify all reported incidents as low, medium, or high risk to facilitate an appropriate response.

Initial Response to a Cyber-Incident

If a potential incident is reported, the Security Team will conduct a preliminary investigation to determine whether a data breach has occurred. If a data breach has occurred, the response team will be notified to follow the investigation checklist set out in the cyber incident response plan to conduct the initial investigation.

The initial response varies depending on the type of incident however, the response team will perform the following at a minimum:

- Stop the cyber-incident or intrusion from spreading further into the company's computer systems.
- Appropriately document the investigation.
- Notify customers, internal stakeholders and the applicable data Controllers.

Coordinating Incident Communication

The Security Team is responsible for coordinating communication with the executive leadership team and other departments regarding cyber-incident issues. While there is overlap of responsibilities among the Executive roles, this Team is responsible for coordinating efforts among all relevant internal corporate departments and ensuring effective communication and cooperation with external parties in response to a cyber-incident and/or data breach. Internal corporate departments include:

- IT
- Human Resources
- Legal
- Each company business unit

External Parties include:

- Regulatory Authorities
- Customers
- Media Agencies

All external communications will be sent by Acumatica to our customers directly. The external communications will include the following points of interest:

- The nature of the data breach.
- The name and contact details of the data protection officer or other contact points where more information can be obtained.
- The likely consequences of the personal data breach.

The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Prepare Legally Required Disclosures

The SEC has advised public companies that they are responsible for evaluating cybersecurity risks and disclosing these risks to investors as appropriate however, Acumatica is a private company, but steps are taken to assess whether the compliance plan and disclosure procedures are required to comply with applicable laws.

Investigating a Cyber-Incident

Following the initial response assessment, Acumatica may decide to undertake a formal internal investigation depending on the level of incident or intrusion and its impact on critical business functions.

An internal investigation allows Acumatica to:

- Gain a fuller understanding of the cyber-incident or intrusion.
- Increase its chances of identifying the incident.
- Detect previously unknown security vulnerabilities.

Identify required improvements to computer systems. In the event of resource constraints or expertise to conduct an extensive internal investigation, Acumatica has established:

- Outside Legal counsel.
- Third-Party Cybersecurity firm on retainer.

Cyber-Incident Response Team

The Acumatica Cyber Security Incident Response Team (“Response Team”) is responsible for investigating and responding to cyber-incidents in accordance with internal stakeholders.

Employee Reporting Mechanism

Acumatica has adopted a reporting mechanism that provides for the Security Team to promptly advise on cyber-incident incidents and can rapidly respond. Employees are made aware of the potential cyber-incidents through either direct notification (specific stakeholders) or companywide.

Acumatica
The Cloud ERP

Acumatica Compliance Work Plan

The Acumatica compliance work plan primarily focuses on monitoring highest risks for potential cyber-incidents. The compliance work plan addresses cyber-incident procedures in addition to other compliance matters. This includes:

- Policies and procedures.
- Codes of conduct.
- Security Awareness Training.
- Specific incident response procedures.

The compliance plan is a living document. The document is reviewed and updated on an ongoing basis.