THE SUBSENTIO WIRE

November 2024

THE LATEST NEWS, VIEWS, & ANNOUNCEMENTS

INSIDE

Information Security
We outline our updated information security program and clarify how we maintain our strategy in a changing cybersecurity landscape while adhering to NIST standards.

Trust & Safety
After a recent FCC settlement, we describe our data destruction policy, ensuring your data is secure and deleted in compliance with security best practices and standard processes.

Corporate News
We are working with a new corporate partner to enhance your experience with our services and implement improvements in our communications and outreach.

CEO Perspective: Spotlight on RE-fined

-By Steve Bock, Founder & CEO

This month, I'd like to highlight RE-fined, one of the charities Subsentio supports in the Denver area. The statistics around human trafficking are not only staggering, but they are also appalling. For example, the average life expectancy of a trafficked minor is only seven years. Runaways are frequently approached for trafficking in less than 48 hours after they leave home.

There are many organizations working to rescue individuals from trafficking situations and get them to a place where they can heal. The healing process is where RE-fined comes in.

RE-fined started with a vision: to restore each survivor's sense of self-worth and value and to empower survivors to live lives of health and dignity. RE-fined partners with law enforcement, rehabilitation homes, and businesses to bring survivors the extra support they need while they are rebuilding their lives. One of the earliest ways RE-fined steps in to help is through the Court Support program, which pairs RE-fined staff members with survivors who are required to confront their abusers in court. The staff member meets with the witness, takes them shopping for professional attire, provides them with salon services, and mentors them through the court process. They also appear in court to support the victims as they give their testimonies.

A recent example of RE-fined's impact on justice occurred on June 6, 2024. In a jury trial, Judge Kandace Gerdes handed down a record 448-year prison sentence to Robert Hawkins after he was convicted on 18 counts—including 5 counts of human trafficking—in Denver District Court. The three cases involved four women, two juvenile girls, and one adult male over several years. One of the juveniles became an adult during the trial. All of the victims testified against the 44-year-old.

The problem of trafficking will only go away if we take action, and you can be a part of that solution! For more information on how to support RE-fined, go to https://re-fined.org/.

Subsentio's Information Security Program Strategy

-By Shawn Hannon, VP of Engineering Services & CISO

Recent enhancements to Subsentio's Information Security Program, including the implementation of authenticator-required multi-factor authentication (MFA) and ongoing employee security awareness training, have strengthened our proactive approach to the ever-changing cybersecurity landscape. This comprehensive, multi-layered defense strategy underscores Subsentio's commitment to protecting our critical assets—data, systems, and personnel—against emerging vulnerabilities, all while adhering to the highest industry standards, such as the NIST Cybersecurity Framework (CSF) 2.0.

These updates are integrated across all levels of our infrastructure—organizational, physical, and technical—while reinforcing robust identity and access management practices. This holistic approach ensures we not only address current risks but also build a forward-looking security posture that safeguards us against future challenges. As the Chief Information Security Officer, I see this evolution as critical to our mission of maintaining operational resilience, securing client trust, and ensuring risk mitigation and compliance across all regulatory frameworks. Our strategy includes:

Organizational Security: Subsentio's security program adopts a proactive, structured approach to managing threats across various sectors. By embedding risk management, access controls, and security awareness into everyday operations, we foster a culture of security-first thinking.

Our commitment to confidentiality, integrity, and availability ensures that only authorized personnel have access to sensitive data. Our employees undergo comprehensive background checks and participate in ongoing cybersecurity training to stay updated on the latest threat trends and mitigation techniques. We have created a security ecosystem where every employee is both a defender and a potential target, underscoring the importance of holistic security awareness.

Physical Security: We have bolstered its physical security measures both at our office premises and data centers. Access to facilities is tightly controlled, with activity logs, camera footage, and visitor logs regularly reviewed. At data centers, two-factor authentication is required, ensuring a secure environment for critical infrastructure. Our measures align with digital security protocols, reflecting a defense-in-depth strategy. This fusion of physical and digital security strengthens overall threat detection and response capabilities.

Infrastructure Security: We maintain a network security architecture designed to mitigate both external and internal threats. Firewalls and strict access control lists are combined with network segmentation to ensure sensitive data and production systems are securely isolated. Additionally, remote access is tightly restricted to secure, authenticated methods, ensuring that network elements remain protected from unauthorized intrusion. The segmentation of our production and development environments is a critical measure in minimizing the impact of potential security breaches, allowing for more targeted responses to incidents.

Data Security: To protect data, we employ state-of-the-art encryption methods, using RSA 2048-bit for asymmetric key encryption and AES 256-bit for symmetric encryption. This ensures that data in transit and at rest remains secure from interception or tampering. We ensure compliance with GDPR and other regulatory frameworks through assessments and audits. Our use of advanced encryption, paired with continuous monitoring of data lifecycle integrity, demonstrates our dedication to reducing risks with data breaches while maintaining compliance across multiple jurisdictions.

Subsentio's Information Security Program Strategy Cont'd

-By Shawn Hannon, VP of Engineering Services & CISO

Identity & Access Control: An identity and access management system ensures that only authorized users can access infrastructure and systems that could contain sensitive data. MFA is enforced using an app-based authentication to access our infrastructure, while a role-based access control (RBAC) policy ensures that users only have the permission necessary to perform their duties. Logs and audits of user access are generated to track all system interactions for security reviews. By integrating MFA and RBAC policies, we not only minimize unauthorized access risks but also create a granular access trail, which serves as a critical tool for post-incident forensics and auditing.

Operational Security: Our operational security framework revolves around constant awareness. Through real-time logging, monitoring, and vulnerability scanning, the company ensures that its systems are continuously protected against threats. Automated tools like Trend Micro and Nessus help proactively identify vulnerabilities, while a 24/7/365 Network Management System (NMS) provides alerts to potential anomalies. Subsentio's use of automated scanning and real-time monitoring provides an edge in incident detection and response, allowing us to quickly contain and mitigate any threats before they escalate.

Incident Response Management: We have a detailed incident response plan that follows the incident life cycle model, including detection, analysis, containment, eradication, and recovery. The program is geared toward minimizing the impact of incidents while ensuring rapid recovery of services. Additionally, Subsentio adheres to strict data breach notification protocols in compliance with regional laws. With a focus on rapid containment and recovery, our incident response plan is designed to ensure business continuity while minimizing the potential reputational and operational damage of security incidents.

Compliance: Subsentio's security strategy is built in alignment with the NIST Cybersecurity Framework (CSF) 2.0, which provides a comprehensive, risk-based approach to managing cybersecurity. By following the NIST framework, Subsentio ensures we meet stringent standards in identifying, protecting, detecting, responding, and recovering from cybersecurity threats. Aligning with NIST CSF 2.0 enhances Subsentio's ability to adapt to evolving cyber threats and regulatory requirements, ensuring that the company stays ahead in a dynamic threat landscape.

Subsentio's enhanced Information Security Program Strategy represents a comprehensive approach to protecting data, networks, and personnel from emerging cyber threats. By leveraging leading frameworks and security-based technology, Subsentio is well-positioned to meet the challenges of today's cybersecurity landscape and deliver robust protection for our clients and operations.

If you have any questions about our security program, please contact us at InfoSec@subsentio.com for more information.

CORPORATE NEWS

New Corporate Partnership

Subsentio is working with a new corporate partner to enhance our client experience and outreach.

We anticipate a formal announcement in the next edition of *The Subsentio Wire*. Look for more information over the next few months on our improved client communications, updated website, and much more!

Trust & Safety: Data Security and Destruction Compliance

-By Gina Alzate, Director of Trust & Safety

As the leading trusted third-party vendor for CALEA compliance, we take data security very seriously at Subsentio, so when we heard about the $13 million settlement between the Federal Communications Commission (FCC) and a major telecommunications company in September, we wanted to outline our existing data destruction policy. We have successfully implemented this policy for the last several years, ensuring our clients were already compliant prior to the FCC settlement.

To protect your company and your customers' data, Subsentio only retains subscriber information for no longer than two (2) years unless otherwise specified by our client. We conduct annual data security and destruction reviews for all our stored customer data, including due process requests, personally identifiable subscriber information, related case management notes, and other required records.

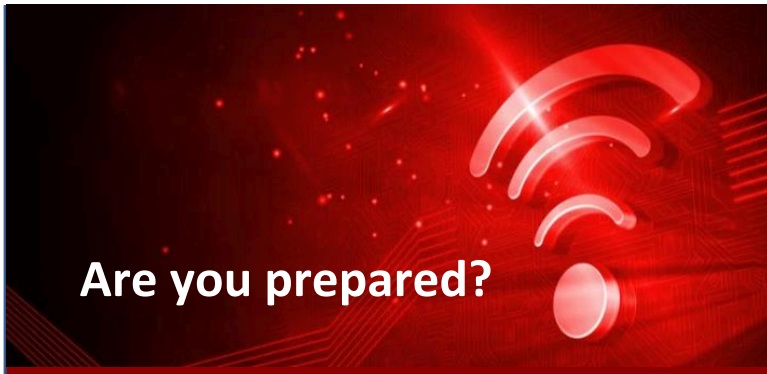
We notify our clients of our data destruction policy and present the opportunity for them to obtain copies of the data. After thirty (30) days, we purge the data from our systems, ensuring that our clients meet the requirements outlined by the FCC in its settlement.

In its settlement, the FCC determined that a security breach occurred when the company's third-party vendor experienced a cloud breach, compromising the security of customer data stored on the vendor's servers. Furthermore, the FCC stated that the vendor retained

the data for several years after it should have been deleted or returned to the company. By neglecting to ensure its vendor adhered to retention and disposal obligations, the FCC determined that the company failed to protect the confidentiality of its customers' data.

The FCC's action sends a clear message to the industry that it will hold companies accountable for failing to protect their customers' data. The $13 million fine is one of the largest penalties ever imposed by the FCC for a data security breach. Fortunately, Subsentio's data security policy already adheres to these requirements, ensuring that you have already been in compliance.

As we approach our annual review, your participation is paramount to its success. We will reach out with more information. If you have any questions, please contact me or our Chief Security Officer, Todd McDermott.



The Montana Consumer Data Privacy Act went into effect in last month, which created new compliance requirements for businesses operating in Montana.

Interested in learning more about new laws and regulations? Contact us at sales@subsentio.com to learn more!