Canon

SECURITY SOLUTIONS AND SERVICES FOR LAW FIRMS

ACS agile cybersecurity solutions Barracuda. SYMPHION

"Most businesses have a probability of 31% of suffering a data breach over the next two years."[1]

Mitigating risk in your firm begins with a comprehensive risk assessment. Canon U.S.A.'s cybersecurity service providers can help you with planning through meaningful consultations. They can also assist with security framework and policy development as well as provide vulnerability assessments and penetration testing to expose any gaps in your firm's security posture.

CYBERSECURITY INTEGRITY AUDITS

Don't leave your practice exposed. Gaps in your firm's security posture left unattended can be an open invitation to malicious cyber criminals who focus on industries such as legal, healthcare, and finance, where the payday for a ransomware attack can be significant. If the corporate clients you represent do business in regulated industries, those regulations my require a qualified third party to run vulnerability assessments and penetration testing routinely to attest that you are doing your due diligence to protect their confidential information. Our Cybersecurity Integrity Audits can assist you with that task.

Assessments to fit any need:

LEVEL 1

Includes an automated scan with a detailed report of findings.

LEVEL 2

Includes an automated scan and also some manual activities with a detailed report.

This option will also include a one-hour debrief via teleconference to explain findings and address any questions.

LEVEL 3

Includes an extensive, all inclusive vulnerability assessment, combination of level 1 & 2 plus a penetration test to demonstrate how an adversary could exploit vulnerability findings.

This would also include a detailed report of findings.

Need more? Request the Advanced Package for an additional six-month follow up Level 1 scan to validate all recommended mitigation has been deployed. It also includes one year of remote phone support for guidance.

[1] *2019 Ponemon/IBM Security Cost of a Data Breach Study*

VIRTUAL CISO

Not all firms have full-time infosec (information security) teams. In today's threat-laden business environment, ignoring the criticality of developing and maintaining a level of security that protects your employees, customers, and intellectual property can lead to catastrophic results. But where do you start?

Your dedicated Virtual CISO (vCISO) can provide expert guidance and services all throughout the cybersecurity lifecycle. They are also adept at working in large firms, assisting established security and IT teams to respond to incidents and can assist in cybersecurity investigations, including cyber forensics. They are equally adept at helping small to medium sized businesses that are just getting started, or in the unfortunate event of an attack, help to mitigate further damage and recover to a normalized state.

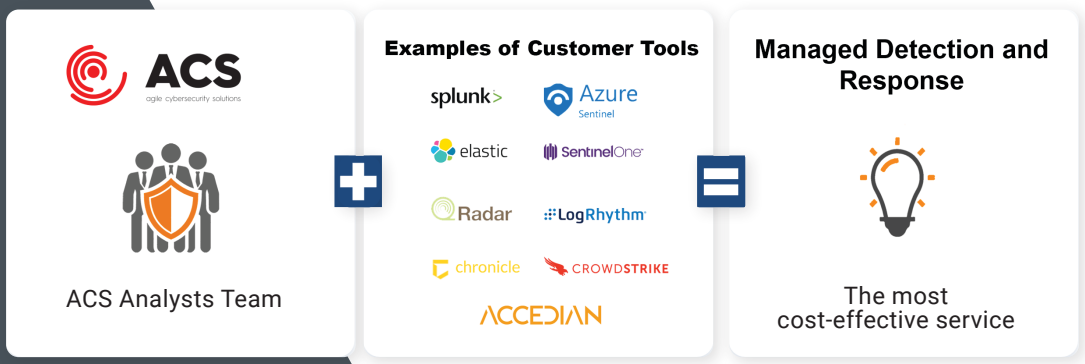
All vCISO services are provided by Agile Cybersecurity Solutions (ACS), a group of seasoned cybersecurity industry professionals, all of whom are credentialed and maintain various levels of security clearances. Virtual CISO Services are twelve-month subscriptions that include 120 hours of discretionary services time. Services also include a 24/7 call center that can alert the ACS team when help is needed in case of a breach or other malicious event. You can choose to dedicate your services to one area of concern or mix and match available services within the ACS portfolio.

General Services Available:

- Analyze the effectiveness of your current security program.
- Assist with risk assessments.
- Coordinate and maintain information security policies, processes, and controls.
- Provide guidance on the acquisition of security products and technologies.
- Establish annual and long-term security goals.
- Develop security and operating procedures.
- Train your staff on security procedures.
- Perform status monitoring and reporting tasks.
- Oversee security breach and incident investigations.
- Oversee External Vulnerability Assessments.*
- Oversee Internal Vulnerability Assessments.*
- Oversee Penetration Testing.*

**The execution of the vulnerability assessments and penetration testing requires the purchase of either the Cybersecurity Integrity Audit or the Cybersecurity Integrity Audit Advanced Package.*

ACS takes your existing tools, tunes them to maximum, and automates response to minimize reaction time and better protect your business.



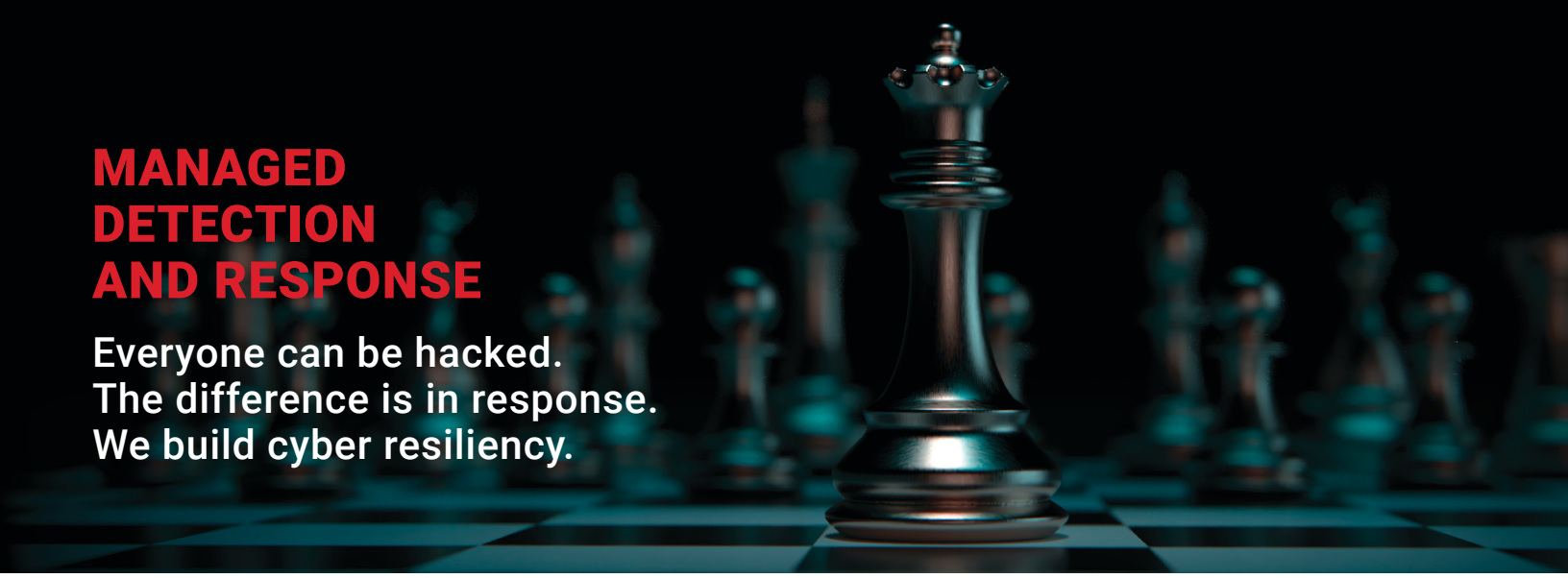
MANAGED DETECTION AND RESPONSE AS A SERVICE

Managed Detection and Response (MDR) is a service that combines continuous monitoring of an organization's digital assets with an "always-on" certified incident response team to defend your network to first prevent, and ultimately to respond to, a cyber-attack.

1. Acquire industry leading expertise to help drive detection and response. The level of competency and experience gained from investigating a range of incidents across different client environments results in a world-class MDR expert team. For a typical enterprise, finding, developing, and retaining this talent is not impossible, but it's often not affordable.
2. Become proactive rather than becoming the attacker's victim waiting to react. Being proactive means to always be vigilant. Detection and response teams fail because they can't escape the constant deluge of activities to which they have to react and respond. MDR as a Service is the way out for shifting in the direction of a proactive security approach. The average industry time of discovery of an incident is 212 days. The average time for IT/Security team to take response action and remediate the threat is 75 days.[2] Attackers will stay undetected in your network, impacting your key assets, IP, code, brand, pricing.
3. Sharing responsibility with your internal security team. Even when an organization has a detection and response team in place, deciding what to prioritize is a challenge. For example, the internal team may focus on external threats but hand off insider threat incidents to an outside firm performing MDR. All MDR services are provided by Agile Cybersecurity Solutions (ACS), a group of seasoned cybersecurity industry professionals, all of whom are credentialed and maintain various levels of security clearances.

40,000
Endpoints Protected by ACS Globally Today

[2] *2021 Ponemon/IBM Cost of a Data Breach Report.*



MANAGED DETECTION AND RESPONSE

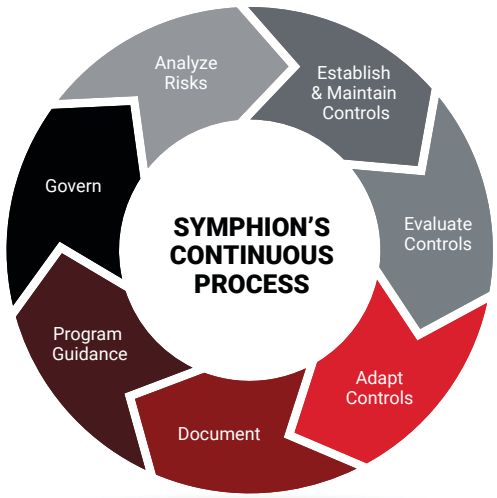
**Everyone can be hacked.
The difference is in response.
We build cyber resiliency.**

WHY MDR AS A SERVICE

When business-critical assets are at risk in today's digital economy, protecting those assets must be of the utmost priority. Increasingly, compliance and regulatory entities require logging and security monitoring be in place. It's no secret that there is a scarcity of skilled cybersecurity professionals, approximately a half a million according to the FBI, which has generated a significant challenge for CIOs and CISOs to identify, hire, and retain top talent to protect their digital landscape.

ABOUT AGILE CYBERSECURITY SOLUTIONS

Located in the Washington, D.C. Metro Area and established in 2012, Agile Cybersecurity Solutions (ACS) has become a trusted leader in the cybersecurity industry. Their unique combination of proven methodologies and multi-disciplined cyber expertise forms a proactive, end-to-end cybersecurity solution. ACS offers the tools and human resources to build a strong defense against the cyber threat, but also to keep you one step ahead of it.



PRINTER FLEET CYBERSECURITY AS A SERVICE™

Canon U.S.A. offers Symphion's specifically designed turnkey Printer Fleet Cybersecurity as a Service (PFCaaS) solution to tackle an often-unaddressed gap in cybersecurity within many law firms today—printers and multifunctional devices. PFcaaS is the only device agnostic printer security management solutions in the industry for firms with hybrid fleets (any brand, any model, any age), period.

Printers – A Hidden Cybersecurity Risk

Printers are the second-most prevalent connected devices on large networks (second only to desktops/laptops). As an often unsecured and unmonitored device on that network, each printer represents not only a threat to the sensitive data that it transmits, processes, and stores, but also many potential open but hidden doorways into and out of the corporate network. Printers can potentially leave your entire network and information vulnerable to theft, ransom, or sabotage.

It Starts with Essential Evergreen Inventory through Device Lifecycle Management and Blueprinting

First, Symphion inventories all the in-scope printers (regardless of make, model, age, or location). This accurate inventory with comprehensive device lifecycle management is maintained throughout the lives of the devices and term of the service. Accurate evergreen inventory is the foundation of all effective Risk Management. Symphion monitors and automatically accounts for changes in inventory and device identifiers such as changes in IP address, device location or configuration, and changes in devices. During the inventory phase, Symphion also blueprints the available (and not available) in-scope security settings/capabilities and the state (e.g., on/off) of each setting/capability on each device.

Essential Testing and Preparation to Avoid Interruptions

In fleets that are not configured for security, they are being managed at a default factory setting level (e.g., published default factory administrator passwords, all ports open). Before turning up the contracted security configuration standard (known as each customer's "Gold Standard") across all printers in the fleet, Symphion follows its proven methodology to test each configuration item to prevent interruptions in use. Symphion's automation tracks and identifies quiet periods (when each printer is not being used) to align testing and turn up periods to avoid interruptions.

Symphion Automation Monitors and Maintains Settings and Alerts

After the Gold Standard controls are set, Symphion automation monitors and maintains those settings. Symphion's highly configurable alerting and event management system offers customers current, historical, and future (trending) visibility to security configuration, inventory, asset management, and firmware-related security events.

Firmware Deployment Service™

Symphion includes its Firmware Deployment Service to bring printer firmware up to each customer's chosen level (e.g., n-1) two times each year of the service for minimum three-year contracts.

Regular Systematic Process with Records Maintained

In addition to monitoring and remediation, our disciplined process automatically establishes a regular risk assessment, a regular security evaluation of chosen controls and historical records of your chosen controls, and measures taken to secure your enterprise. These records are readily available for auditors without requiring a project or your employees' time. Our process and records match most security mandates for regular assessment and record keeping including NIST RMF, HIPAA Security Rule, and others.

SYMPHION PRINTER FLEET CYBERSECURITY AS A SERVICE BENEFITS

No FTEs or Projects Required

Just as with electrical service being provided to your business or home, your employees are not required to be involved in delivering this valuable service. There are no projects required to implement, upgrade, or administer the solution. Your Symphion concierge team will take care of it all.

No Agents to Install

All Symphion solutions are agentless. There is no software to install on target devices to enable scanning. No software to interrupt the operations of your other systems.

No Hidden Costs: Fixed Fee Pricing – Adjusted (Right-Sized) and Predictable

Symphion is focused on returning the highest value to customers and providing predictable pricing. To do this, pricing is fixed based on the number of in-scope devices (with minimums).

Solutions are Deployed on Your Infrastructure, Inside Your Firewall

Symphion's "as a Service" solutions are all deployed on the customer's virtual servers and hosted in the customer's datacenters. No data leaves your premises, thereby providing the most secure deployment.

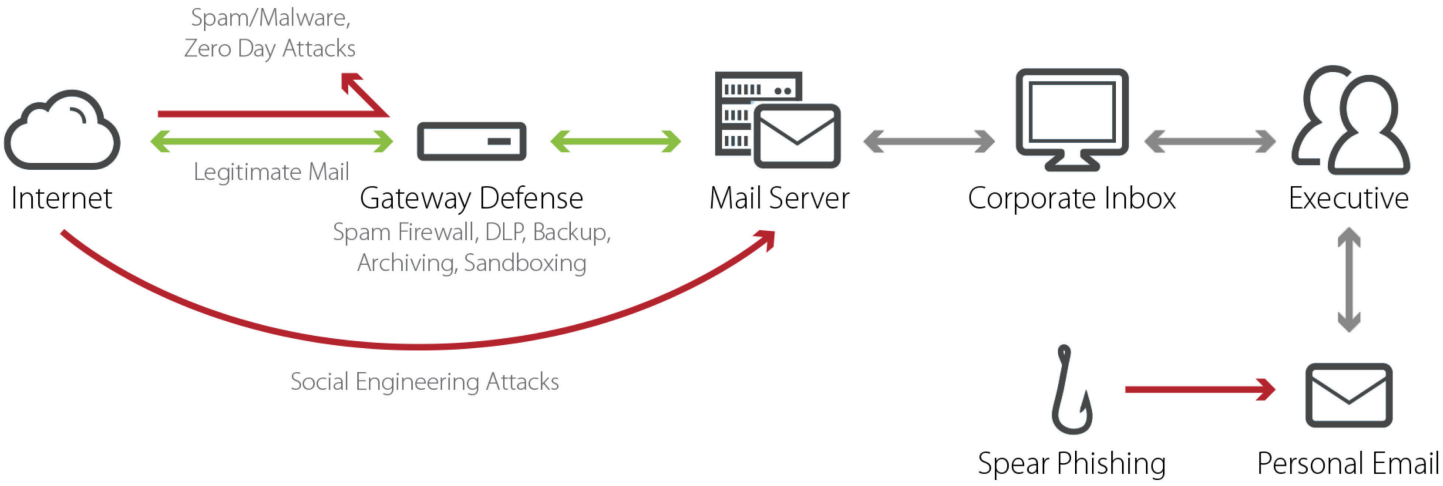
ABOUT SYMPHION

Symphion, Inc. is a Dallas, Texas based software and services company focused on continual innovation, seamless delivery, and dedication to excellence in customer service. Their unique "as a Service" solutions are designed to provide effortless delivery of actionable information and results to eliminate cost and risk and to increase operational efficiency.

TOTAL EMAIL PROTECTION

Secure email gateways are no longer enough to defend against today's sophisticated social-engineering attacks. These attacks bypass traditional security and end up costing organizations time, money, and brand equity.

Barracuda Email Protection is the most effective solution to prevent targeted social-engineering attacks. Its multi-layered approach combines a secure email gateway, AI-powered fraud protection, and advanced security awareness training.



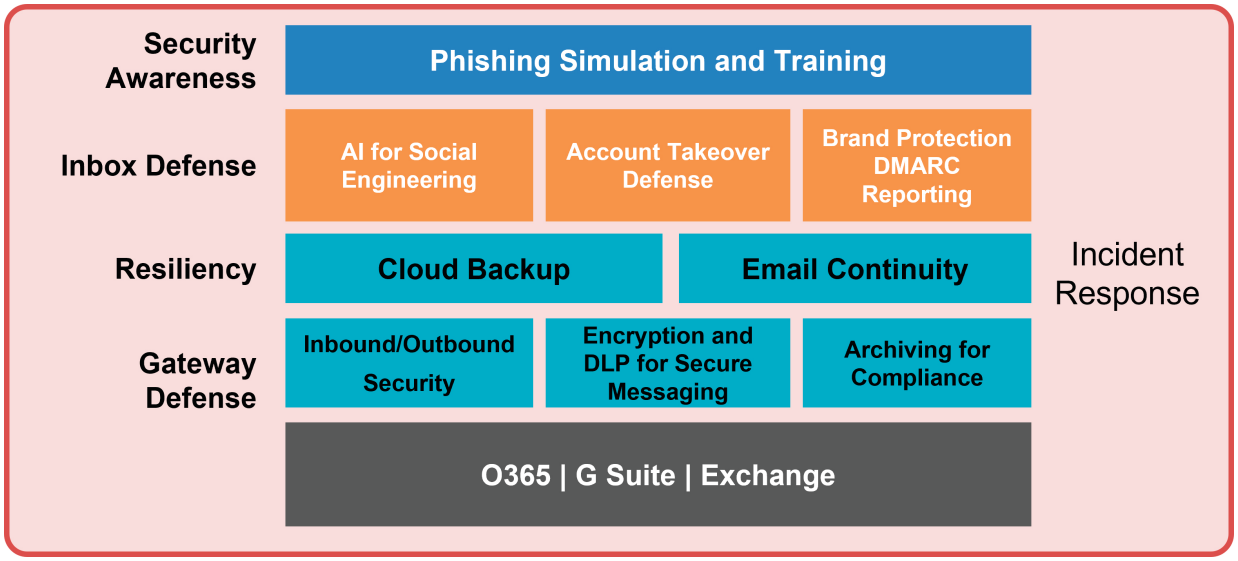
The Human Factor

Social engineering accounted for over 80% of data breaches in 2021[3], with Phishing leading the pack. Also in the mix were Business Email Compromise (BEC) and Pretexting. The study also showed that cost-wise, those organizations that deployed Artificial Intelligence (AI) in their security mix had a significantly lower cost per breach. As much as 80% less:

- With AI $2.90 million
- Without AI $6.61 million

A Layered Approach

Your practices' staff can either be your best defense or your weakest link. In addition to routine security awareness training with social engineering simulation campaigns, Barracuda offers infrastructure solutions that help to automate inbox protection with tools like Barracuda Sentinel for Microsoft 365, with AI that learns patterns of malicious activity and malware in staff inboxes. Protecting your firm's email infrastructure requires a layered approach.



[3]*2021 Verizon Data Breach Investigative Report*

Barracuda Total Email Protection

Barracuda Protection Plans
Comprehensive security and data protection for Microsoft 365©, Barracuda Protection Plans let you migrate to Microsoft Office 365 safely, efficiently, and economically. There are three plans: Advanced, Premium and Premium Plus. From basic gateway protection and DLP all the way to providing security awareness training that helps protect your users and your organization from dangerous ransomware and phishing attacks.

Barracuda Impersonation Protection and Domain Fraud Protection
Artificial intelligence for real-time email protection. Business email compromise (BEC), spear phishing, and account takeover are today's top email threats. These hyper-targeted attacks trick employees into making terribly costly mistakes. Barracuda Sentinel combines artificial intelligence, DMARC, deep integration with Microsoft 365, and brand protection into a comprehensive cloud-based solution that guards against these potentially devastating attacks.

Barracuda Security Awareness Training
Fight phishing with continuous simulation and training. Barracuda Security Awareness Training teaches users to understand and respond correctly to the latest phishing techniques, recognize subtle phishing clues, and prevent email fraud, data loss, and brand damage. It transforms employees into a powerful line of defense against damaging phishing attacks. This versatile, scalable, cloud-hosted SaaS solution includes hundreds of email and landing page templates, kept up to date based on threat trends. Levelized training and gamification make it more effective by engaging employees.

Incident Response Complements Email Security

So how can Barracuda's Incident Response help? Your firm's users will continue to report incidents as they come in. In addition to that, you can also use insights from forensics to find anomalies in delivered mail and speed up your own investigations. For example, administrators can access a visual report that shows where email is coming from, what countries it originates from. If most of their business and email comes from North America and they notice a couple of emails originating from Nigeria, they can quickly review and determine if the email is legitimate.

Once malicious email is identified, administrators can use Barracuda to quickly search through their email servers to identify other messages from the same sender or with the same subject line. The search will return all associated emails and users that received them. This takes only a few seconds and saves a lot of valuable time. Once all malicious emails are identified, admins can create incidents and move to remediation.

Remediation is very fast and easy. With a couple of clicks, admins can automatically send alerts to all impacted users and quarantine messages directly from the users' inboxes.

SECURITY AWARENESS TRAINING

The Department of Homeland Security insists: "Security is everyone's responsibility." But your staff does not know what they don't know. Social engineering has been responsible for many of the most catastrophic ransomware attacks and data breaches in recent times. One click on a nefarious link or a malicious file attachment download could surely result in disaster.

Security awareness training to improve user behavior for email and internet usage habits is not a one-and-done event. It must be routine and consistent for those habits to improve.

Introducing Barracuda Security Awareness Training

When it comes to threat mitigation, the reality is that your people are either the weakest link that cyber criminals are looking to exploit through social engineering, or they can be your best defense if they are made aware in a consistent manner and in a meaningful way. There is no more important element in a successful security posture than employee awareness. Some of the most catastrophic data breaches in recent history were the result of an insider being exploited by an email phishing attack.

What is Phishing?

Phishing is a technique used by hackers to impersonate a trustworthy entity in an email. Attackers use phishing emails to obtain sensitive information such as usernames, passwords, or banking credentials. They distribute malicious links and attachments to trick users into downloading malware or ransomware. These attacks are usually sent in large numbers to business users and consumers—at random— with the expectation that only a small number will respond.

The Barracuda Advantage

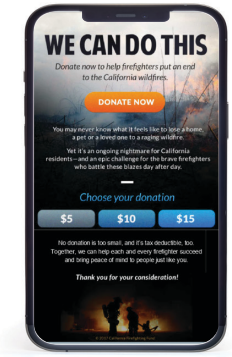
- Protect your firm with a versatile, scalable, cloud-based SaaS solution.
- Guard against a range of threats with patented, highly variable attack simulations for Phishing (Email), Smishing (SMS), Vishing (Voice), and Found Physical Media (USB/SD Card).
- Train users with comprehensive, SCORM compliant courseware.
- Get industry-leading analytics and reporting.
- Take advantage of program and address book automation.

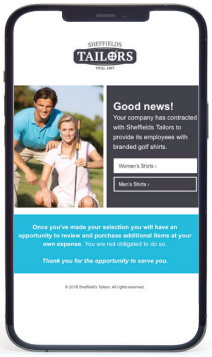
Product Spotlight

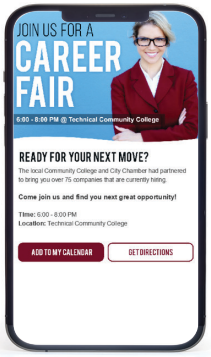
- Choose from hundreds of email templates, landing pages, and domains.
- Automatically direct training and testing with the built-in workflow engine.
- Make it easy for users to instantly report suspicious emails with the Phish Reporting Button.
- Embed learning into your everyday business processes.
- Test and reinforce good behavior.

Simulation Campaign Content

Barracuda refreshes the simulation content monthly to keep the training fresh so that users don't become complacent. The content includes emails, websites, social media pages, etc. Below are some generic examples:





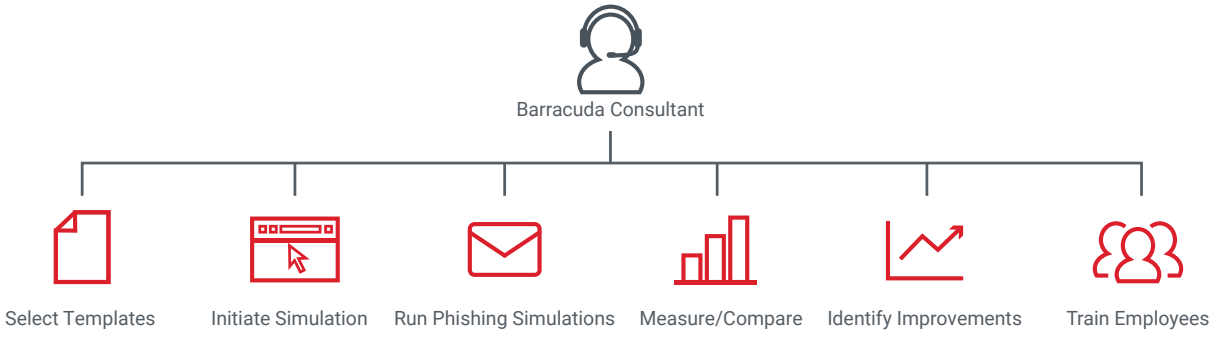


Measuring Success

The Security Awareness dashboard allows campaign administrators to keep a careful eye on who is doing well and who needs a bit more guidance. Some organizations use a reward system and gamification techniques to get workers to buy in and motivate them to retain the information in the simulation exercises.

Security Awareness Training Concierge Service

Barracuda is unique among other security awareness training programs in the market today, in that they offer a "Concierge" service option. For those practices that don't have adequate workforce to dedicate a campaign administrator, Barracuda can provide a dedicated subject matter expert who will design, execute, and measure the campaigns over the course of the annual subscription.



ABOUT BARRACUDA

More than 200,000 global customers trust Barracuda to safeguard their employees, data, and applications from a wide range of threats. Barracuda provides easy, comprehensive and affordable solutions for email protection, application and cloud security, network security and data protection. Barracuda is continually innovating to deliver tomorrow's security technology, today.

THE CANON U.S.A. 5 PILLARS OF SECURITY

The Canon U.S.A. Five Pillars of Security focus on the fundamental security principles of Confidentiality, Integrity, and Availability. The services and solutions that have been featured in this brochure are all part of our layered approach to helping our customers protect their law practices in five key areas:

Device Security

- Authentication
- Role-based Access
- HD Overwrite
- HD Encryption
- Network & Protocol

Document Security

- Secure Storage
- Encryption
- Role-based Access
- Copy-lock

Cybersecurity

- Consultation
- Assessments
- Penetration Testing
- GDPR Prep
- Incident Response
- Virtual CISO
- Training & Awareness

Print Security

- Authentication
- Pull Printing
- Encryption *(in transit and at rest)*
- Keyword Intercept
- Auditing

Information Security

- File Encryption
- Access Control
- Tracking & Auditing
- Data Loss Prevention

Canon

1-844-50-CANON | usa.canon.com/security

11/25-0173-6450