MIKE BRANGWYNNE

Cybersecurity Manager

[redacted]

[redacted]

[redacted]

linkedin.com/in/michael-brangwynne

cybermike.io

Cybersecurity Solutions

Firewalls

- Cisco Firepower
- Cisco Meraki

Next Generation Anti-Virus and Endpoint Detection & Response (NGAV/EDR):

- Crowd Strike
- Carbon Black
- McAfee
- Kaspersky
- Sophos

Intrusion Detection and Prevention Systems (IDS/IPS)

- Arctic Wolf
- Cisco Firepower
- Snort
- Alien Vault

Security Information and Event Management (SIEM)

- Splunk
- Log Rhythm
- Arctic Wolf
- Dragos (OT Environments)

Identity and Access Management (IAM)

- Microsoft Azure Active Directory
- Zscaler
- Bomgar (Beyond Trust)
- SurePassID
- Duo 2FA

Data Loss Prevention (DLP)

- Crowd Strike
- Microsoft 365 DLP

Email Security

- KnowBe4
- Mimecast
- Barracuda Email Security
- AppRiver

Vulnerability Assessment and Management

- Crowd Strike
- Qualys
- Tenable Nessus
- Rapid7

Encryption and Data Protection

- Symantec Data Loss Prevention
- ESET Endpoint Encryption
- Microsoft Intune

Summary

Dedicated and experienced **Cybersecurity Manager** with a proven track record of safeguarding organizations against cyber threats. Excels in spearheading IT Cybersecurity initiatives, driving the implementation of cybersecurity enhancements, and optimizing system efficiencies. Possess a strong track record of effectively identifying, assessing, and resolving vulnerabilities through the use of cybersecurity platforms while establishing new procedures to consistently deliver high-quality results. Seeking to leverage my expertise in developing and implementing robust cybersecurity strategies to protect sensitive data and enhance IT security.

Professional Experience

2020 - Current

Senior Cybersecurity Administrator

NECI

Cybersecurity Department Lead and managed an internal team of cybersecurity analysts. My responsibilities encompassed both internal security measures to protect the company from cyber threats and external engagement for customer cybersecurity solutions and sales.

- Played a central role in establishing comprehensive company-wide cybersecurity governance, which included formulating and implementing Cybersecurity Policies and Procedures.
- Successfully oversaw the full deployment of all corporate cybersecurity platforms and implemented robust incident response procedures.
- Responsible for the design and implementation of tailored cybersecurity offerings, including software and services, to cater to the specific needs of our customer cybersecurity programs.
- I effectively managed and completed all external cybersecurity audits and assessments.
- Crafted a corporate cybersecurity strategy with a strong emphasis on a "cybersecurity mesh" and a "defense in depth" approach, fortifying the company's cybersecurity measures.
- Elevated corporate cybersecurity governance by developing IT Cybersecurity Policies and Procedures, providing clear cybersecurity guidelines for the organization.
- Introduced a comprehensive employee cybersecurity training program, along with supplementary training and monthly phishing email assessments, resulting in a remarkable reduction in the company's Phish-prone percentage from 42.8% to 3.3%.
- Spearheaded the creation and launch of a cybersecurity ticketing system, streamlining alert processing and enhancing executive-level reporting.
- Innovatively developed a Cybersecurity Communication page within the existing Employee hub (SharePoint) to facilitate the dissemination of Cybersecurity Alerts, Announcements, News, and the sharing of cybersecurity documentation across the company.
- Significantly enhanced the corporate security posture by implementing new corporate Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), Unified Endpoint Management (UEM), Privileged Access Management (PAM), and Multi-Factor Authentication (MFA) solutions.
- Enforced new Data Loss Prevention (DLP) Policies to safeguard against corporate and protected data loss.
- Orchestrated the implementation of a new IT Change Management process, ensuring the proper identification of change impacts and risks to the company.
- Led the organization and establishment of a new company Incident Response Team, including the development of an Incident Response Policy and Plan.
- Took the lead in customer cybersecurity-related engagements, contributing to the development of innovative, customer-focused cybersecurity solutions and services.
- Successfully defined and achieved Objectives and Key Results (OKRs), surpassing revenue targets for customer cybersecurity sales by more than threefold.

2019 - 2020

Network Administrator

Princess House

Managed Network and Security Administration responsibilities for the company's primary office and main product distribution facility. Additionally, played a key role in overseeing company backups at on-premises locations, an external backup site, and cloud-based backup repositories. Provided support for high-tier help desk tickets escalated through the help desk ticketing system. Led the comprehensive development of IT Department Policies to facilitate company auditing for PCI-DSS Compliance.

Mobile Device Management (MDM) and Mobile Security/ Unified Endpoint Management (UEM)

- Microsoft Intune
- VMware Workspace ONE
- Sophos
- LanSweeper

Backup and Recovery

- Veeam

Password Managers

- BitWarden
- LastPass
- Dashlane
- Keeper

Priveledged Access Management (PAM)

- Admin By Request
- Thycotic Secret Server

Virtualization

- VMWare ESXi
- VMWare VSphere
- OCI - Oracle Cloud Infrastructure
- AWS
- Any.Run (virtual sandboxing)

Patch Management

- PDQ Deploy
- Manage Engine Patch Manager
- Microsoft Intune

Company Involvement

- **BCP Deputy Leader** –Took one of the leading positions for Business Continuity Plan's IT Systems Team.
- **5S Audit Team** –Part of companies health and safety 5S Audit team responsible for maintaining, understanding and grading company standards for workplace organization.
- **Food Service Team - Company team to establish new expanded company food options.**

Activities

- **Golf Team Committee** –Worked in Company Golf League as a decision maker, season score tracker and schedule development.
- **Kids Christmas Party** –Assisted in organizing, planning and decorating for the company's Kids Christmas party every year.

- Implemented and configured a visitor registration and badge system for the front desk.
- Took the lead in managing company Patch Management through the utilization of Manage Engine Patch Manager.
- Maintained the entire Microsoft Office 365 Suite for the company, including the successful implementation of Multi-Factor Authentication (MFA) for all user accounts.
- Oversaw the configuration and implementation of the new cloud email security platform, Mimecast, and email security policies within Office 365.
- Contributed to the rollout of the company's new Security Information and Event Management (SIEM) system, Logrhythm.
- Implemented, configured, and ensured the maintenance of Sophos Central for anti-virus protection, server security, device encryption, and Intercept X.
- Developed a comprehensive Governance, Risk Management, and Compliance (GRC) Training and Testing program using KnowBe4, incorporating PhishER email reporting tools.
- Assisted in configuring and maintaining company backups using Veeam, encompassing on-site physical tape backups, off-site backup locations, and cloud-based backup repositories.
- Initiated the creation of all nine company IT policies to align with PCI-DSS Compliance requirements and participated in the annual company audit for compliance validation.
- Led the implementation, configuration, and user training for Microsoft Teams, facilitating its deployment across the entire company, which included the migration of departmental shared documents from an on-site server to OneDrive.

2015 - 2019

IT Specialist

Senior Aerospace Metal Bellows

Assumed a leadership role in overseeing the company's IT Ticketing System, where I personally managed all user-submitted tickets and served as the primary point of contact for resolving workstation issues. Independently handled task prioritization, hardware and software procurement aligned with company requirements, and skillfully scheduled and organized the timely execution of both ongoing and upcoming departmental tasks.

- Managed the company's intranet site (SharePoint Foundations) with a focus on standardizing the conversion of all company Human Resources forms into electronic format.
- Successfully installed and configured company asset monitoring software (LanSweeper) and integrated it with the company's IT Ticketing System.
- Efficiently configured and installed both End User and Server Antivirus Software (Kaspersky and ESET), implementing automated scheduling for scanning, updates, and installations.
- Played a pivotal role in the company-wide deployment of Multi-factor Authentication Token Cards (SurePassID), Symantec Endpoint Encryption, and AirWatch to ensure compliance with Federal ITAR/NIST/DFARS Regulations.
- Contributed to upgrading the company's Exchange Server, Microsoft Office Software, Cisco Phone System Hardware, Barracuda Web Security Gateway, and the implementation of Port Security on Cisco Switches.

2021 - 2021

CompTIA Security+ ce Certification

CompTIA

Cybersecurity role certification from CompTIA

2020 - 2020

MCSA: Microsoft Certified Server Administrator

Microsoft

Microsoft Server 2016 Certification

2003 - 2008

Bachelor's Degree in English: Writing, Communications and Rhetoric

University of Massachusetts Dartmouth

Received degree with a focus in Online Marketing and Online Advertising