Acronis

A Checklist for Implementing Cyber Protection for SMBs

Cyber Protection Checklist

Legacy protection technologies lack integration. Cyberthreats are on the rise. Breaches happen more often and on more devices.

When it comes to cybercrime, today's small and midsize businesses (SMBs) are an easy target. Budgets and staffing are limited, and finding the right skilled people is difficult. Many opt to rely on a managed service provider (MSP) to administer their IT needs and keep their workloads and systems secure.

However, since the cyberthreat landscape is always evolving, many MSPs also struggle to stay ahead of new threats. In fact, cybercriminals have successfully attacked the platforms that service providers use to run their businesses to gain access to both the MSPs' data and their clients'.[1]

A backup and restore strategy alone is no longer sufficient to keep data safe.[2] The objective of new ransomware strains is to delete backup files, agents, and security software. Backup without integrated cybersecurity capabilities is not enough.

A new approach

A new approach is needed — one that efficiently integrates cybersecurity, data protection, and endpoint protection management. Integration enables strict control and interlocked automation that legacy solutions lack but are required to combat today's threats.

And, while there are many cybersecurity frameworks, such as NIST, COBIT, and CIS, available to provide industry standards and best practices for organizations to manage their cybersecurity risks, they are complicated.

By integrating cybersecurity and data protection — the **IT discipline of cyber protection**[3] according to IDC — organizations become more resilient.

Cyber protection integrates backup, disaster recovery, AI-based anti-malware, remote assistance, and cybersecurity into a single, fast, efficient, and reliable tool. With the five stages below, you can proactively protect data from today's advanced threats.

- **Prevention** — Proactively protect your data, systems, and applications by preventing attacks from happening in the first place
- **Detection** — Detect issues and threats before they pose a risk to any environment
- **Response** — Enable quick action to minimize risk
- **Recovery** — Quickly and safely restore data from known, accurate backups in the event it gets compromised
- **Forensics** — Mitigate future risks by collecting and performing forensic investigations

You can begin planning and benchmarking your cyber protection posture and potentially achieve lower risk with this checklist.

> "Bolting security onto an information technology system after its creation generates challenges that are often more costly to address than if security was baked into the development process from the outset." [4]
>
> **Tanner Johnson**
> **Senior Analyst Connectivity**
> **& IoT Omdia, Informa PLC**
> Helping you connect the dots across
> the technology ecosystem

PREVENTION

Proactively protect your data, systems, and applications by preventing attacks from happening in the first place.

	Element	Current Status	Improvement Plan
1	**Vulnerability assessments** To remediate or mitigate potential risks, systematically review security weaknesses in information systems.		
2	**Patch management** Patching known vulnerabilities minimizes the risk surface exposure of an organization. Patch management rollbacks have limitations and can be slow. Create an image backup of selected machines before installing a system or application patch.		
3	**Data loss prevention (DLP)** Monitoring and blocking sensitive data while in use and at rest will prevent potential data breaches and transmission to bad external actors.		
4	**Security Awareness Training** Often how prepared staff is to meet cyberattacks and follow internal processes with security in mind determines the safety of corporate data.		
5	**Self and collaboration tools protection (Zoom, Webex, Teams)** Self-defense and hardening rules for specific applications help extend protection to all critical applications, especially those remote devices.		

Do your endpoint security solutions proactively scan backups for viruses, vulnerabilities, and patch level to prevent re-infection?

DETECTION

Detect issues and threats before they pose a risk to any environment.

	Element	Current Status	Improvement Plan
1	**Antivirus and anti-malware** A combination of AI- and behavior-based detection will protect from both traditional and next-generation forms of intrusion, like zero-day attacks.		
2	**Anti-phishing** When end-users don’t recognize a phishing email, security measures may prevent or block phishing attempts from entering an organization’s email system or from succeeding in stealing information from the user.		
3	**URL-filtering** Control access to the internet by permitting or denying access to specific websites based on information contained in a URL category list.		
4	**IoC-based detection** Check against a known list of compromise attributes if evidence on a computer or network indicates that the network’s security has been breached.		
5	**Endpoint detection and response (EDR)** EDR combines real-time continuous monitoring and collection of endpoint (computer hardware devices) data with rules-based automated response and analysis capabilities.		

Does your cybersecurity stack include automated generation of allowlists from backups?

RESPONSE

Enable quick action to minimize risk.

	Element	Current Status	Improvement Plan
1	**Block malware execution** Protect users from inadvertently executing malicious files and script files, including those like file-less attacks that don't write files to the disk.		
2	**Device isolation** Prevent devices connected to a network from accessing other resources connected to the same or other networks once a compromise has been identified.		
3	**Incident response** How quickly and effectively an organization responds to data breaches will determine the financial and reputational damage it faces.		
4	**Alerts and notifications** These provide timely information about current security issues, vulnerabilities, and threats.		
5	**Network security** Centralized management of network security infrastructure will enable visibility into network-wide traffic and threats to secure access, protect users and applications, and control data from anywhere.		

Does your existing stack automatically adjust protection levels and begin backups based on security alerts?

RECOVERY

Quickly and safely restore data from known, accurate backups in the event it gets compromised.

	Element	Current Status	Improvement Plan
1	**Remove malware from backup** Scanning full-disk backups at a centralized location helps find potential vulnerabilities and malware infections – ensuring users can restore a malware-free backup.		
2	**Instant "in-place" recover affected data** Instant recovery allows a backup snapshot to run temporarily as a virtual machine (VM) on secondary storage after a failure or disaster occurs.		
3	**Safe recovery** Patching the machine and applying the latest anti-malware definitions allows users to restore the OS image with the latest patches, reducing the chance of a reoccurring infection.		
4	**Automation** Having the ability to configure all workflow areas automatically - at a process, application, or infrastructure level - reduces manual dependencies.		
5	**Email archiving and recovery** Preserve and keep or recover business-critical emails.		

How confident are you that you are recovering from clean backups?

FORENSICS

Mitigate future risks by collecting and performing forensic investigations.

	Element	Current Status	Improvement Plan
1	**Full data backups** Capture all data from source devices (computers, cell phones, tablets, etc.) forensically so that all original data is in an unaltered state.		
2	**Forensic data in backups** Capture a memory snapshot including the state of all running processes together with the backup.		
3	**EDR** Perform root cause analysis to identify the origin of compromise and infection path.		

Does your forensics system have access to backups to help with incident response analysis?

Harness the Power of One

Proactively protect your clients' business data from today's advanced threats with the five stages of cyber protection.

Learn more at:
https://www.acronis.com/cyber-protection/

Acronis is the only solution that natively integrates backup, disaster recovery, AI-based anti-malware, remote assistance, and cybersecurity into a single, fast, efficient, and reliable tool.

References

[1] Cybersecurity for SMBs Is the Herculean Task of MSPs, Dark Reading, November 2020

[2] Ransomware protection means more than a simple backup, Omdia, March 2021

[3] Addressing Cyber Protection and Data Protection Holistically, IDC, April 2020

[4] Data Security Strategies Are at the Heart of Cybersecurity, Omdia, Tanner Johnson, October 2020

Acronis

Learn more at
www.acronis.com