SCHNEIDER DOWNS

Big Thinking. Personal Focus.

10 Things Companies Wish They Did Before a Breach

A Strategic Guide to Breach Preparation

10 Things Companies Wish They Did Before a Breach

A Strategic Guide to Breach Preparation

In the aftermath of a cybersecurity breach, organizations identify critical gaps that could have dramatically reduced their impact, recovery time, and overall costs.

This guide shares decades of response team experience and post-incident analysis, highlighting 10 of the top preparations companies wish they'd implemented before a breach.

These aren't exotic technologies; they're proven practices that transform organizations from reactive to proactive security postures. These preparations represent the difference between a manageable incident and potential business-threatening catastrophes.

1. Incident Response Team

Organizations must establish a dedicated incident response team with clearly defined roles, responsibilities, and decision-making authority. This team coordinates response efforts and makes critical decisions under pressure, with clear escalation paths preventing confusion during crises. The team should include key stakeholders covering these roles:

- **Incident Commander:** Tactical leader and strategic decision maker
- **Security Lead:** Coordinates security-specific efforts, such as forensic analysis
- **IT Lead:** Coordinates technical efforts across system administrators and engineers
- **Communications:** Manages all internal and external communications
- **Legal Counsel:** Advises on legal risks and requirements, such as breach reporting
- **Scribe:** Records all response activities for insurance and post-incident review

Organizations should tailor their team roles to best fit their organization and then designate primary and backup personnel for each role, ensuring 24/7 coverage capability.

2. Incident Response Plan (IRP)

A written IRP provides step-by-step procedures, decision trees, and resource inventories that enable a coordinated response rapidly without wasting critical time resolving conflicting approaches under pressure. Key focus areas include:

- **Decision Matrix:** Clear authority levels and approval processes
- **Contact Information:** Current details for team members, vendors, and authorities
- **Incident Classification:** Severity levels and escalation criteria
- **Response Procedures:** Step-by-step actions for different incident types
- **Communication Templates:** Pre-drafted notifications for various stakeholders

An effective IRP should include input from all relevant stakeholders and be specific enough to guide action, yet flexible enough for unique circumstances.

3. Tabletop Exercises

An untested IRP may be unhelpful when needed most. Regular testing reveals gaps, builds team competence, and transforms procedures into practiced capabilities.

Effective testing progresses scenario complexity over time to gradually build team capabilities and confidence. Tests should include practical aspects of scenarios, such as password changes or network isolation steps. Post-exercise reviews identify lessons learned and drive plan improvements.

4. Cyber Insurance

Cyber insurance has evolved from a convenience to an essential risk management tool. Beyond financial protection, modern cyber insurance policies provide access to specialized incident response resources, legal expertise, and recovery services that many organizations cannot maintain in-house.

Organizations should carefully assess coverage limits, exclusions, and requirements. Many policies mandate specific security controls and preparedness measures, creating positive reinforcement for good cybersecurity practices. Regular policy reviews ensure coverage keeps pace with organizational growth and evolving threat landscapes. Misrepresented controls in cyber insurance application/renewal forms can result in denied claims.

5. Pentesting

Penetration testing simulates sophisticated attacks to provide actionable intelligence that enables risk-based prioritization over theoretical severity scores. Organizations should go beyond compliance and perform preventative assessments to identify exploitable vulnerabilities, exceptions and attack paths for prioritized remediation.

Regular testing establishes security maturity baselines, demonstrates ROI to executives, and transforms cybersecurity from a cost center to a competitive advantage while strengthening insurance and compliance positions. By revealing vulnerabilities before attackers find them, validating controls under realistic conditions, and building response capabilities, strategic penetration testing helps organizations thrive despite cyber threats.

6. Logging, Alerting, and Detection

Logs provide the digital forensic foundation for incident investigation, informing response efforts. Without proper logging, organizations operate blindly during critical moments. Settings should be adjusted from defaults to increase log details and volume to include:

- **Network Traffic:** Firewalls, routers, switches, intrusion detection systems
- **System Logs:** Operating systems, applications, databases, cloud services
- **Security Logs:** Authentication systems, VPN connections, security tools
- **User Activity:** File access, email systems, web browsing, application usage

Active monitoring transforms data into actionable intelligence for early threat detection and rapid response. Success requires tuned detection rules, balanced alert thresholds, and trained personnel to reduce blind spots and minimize false positives.

7. Vendor Retainers

Pre-existing partnerships can dramatically reduce response times by eliminating vendor selection, contract

negotiations, and relationship building during crises. Established relationships enable immediate protocol activation, instant access to specialized expertise, and clear communication channels, transforming hours of setup time into an immediate coordinated response. Relevant partnerships include:

- **Digital Forensics and Incident Response:** An incident response team on retainer can expedite evidence collection and triage to quickly inform containment efforts
- **Legal Counsel:** Legal counsel with adequate cyber expertise and familiarity with the organization can quickly guide regulatory compliance and breach notifications
- **Law Enforcement:** Information sharing with law enforcement contacts can help agencies build a case against the threat actor and provide a variety of assistance
- **On-Demand Managed Service Provider (MSP):** Scalable support from an existing MSP, as needed, can be helpful to enable recovery efforts, such as restoring or rebuilding many systems

Contact lists should be maintained by an assigned handler and documented in the IRP.

8. Secure Backups

A robust backup strategy serves as the ultimate insurance policy against data loss, from cyber attacks,

system failures, or human error. Modern backup strategies must account for sophisticated attackers targeting backup systems to maximize extortion leverage.

- **3-2-1 Rule:** Three copies of data, on two different media types, with one offsite
- **Air-Gapped Backups:** Physically or logically isolated backup copies
- **Immutable Backups:** Write-once storage that cannot be modified or deleted
- **Routine Testing:** Regular validation of backup integrity and restoration procedures

Effective backup strategies balance recovery objectives with cost and complexity considerations. Organizations must define recovery time objectives (RTO) and recovery point objectives (RPO) for different data types and systems. Regular restoration testing ensures backups function correctly when needed most.

9. Backup Communications

Threat actors often target communication infrastructure first to prevent a coordinated response. Organizations with pre-established backup channels—satellite phones, secure mobile networks, or radio systems—can maintain critical coordination between teams, leadership, and external partners, often determining whether incidents remain manageable or escalate catastrophically.

Emergency communication capabilities enable organizations to control their narrative through timely stakeholder updates rather than allowing speculation. This proactive approach maintains confidence, demonstrates resilience, and can strengthen reputation. Organizations that communicate clearly throughout crises typically recover faster and gain enhanced credibility.

10. Controls Framework

Organizations should implement a comprehensive risk-based strategy for security controls. Security frameworks, such as NIST-CSF, ISO 27001, and CIS Controls, help ensure best-practice controls by providing a structured approach to cybersecurity management, focusing on comprehensive coverage of essential security domains while enabling consistent measurement and improvement. Examples of high-priority controls enforced by industry-leading frameworks:

- **Multi-Factor Authentication:** Prevents credential-based attacks
- **Endpoint Protection:** Detects and blocks malware on devices
- **Network Segmentation:** Limits attack propagation and blast radius
- **Access Controls:** Ensures appropriate permissions and regular review

Framework selection and control implementation maturity should align with organizational needs, industry requirements, and available resources.

From Regret to Resilience

The question is not whether an organization will face a cyber incident, but whether they will be prepared when it happens. These 10 preparations are the collective wisdom of organizations that have experienced cyber incidents and emerged stronger. Their regrets have become our roadmap to thrive in an increasingly digital world where cybersecurity resilience has become a defining characteristic of successful enterprises. The best time to implement these controls was yesterday. The second-best time is today.

How Can Schneider Downs Help?

For more information about implementing these cybersecurity preparations in your organization, or to access additional resources and tools, please contact our cybersecurity consulting team at **cybersecurity@schneiderdowns.com**.

About Schneider Downs Cybersecurity

The Schneider Downs cybersecurity practice consists of experts offering a comprehensive set of information technology security services, including penetration testing, intrusion prevention/detection review, ransomware security, vulnerability assessments and a robust digital forensics and incident response team. In addition, our Digital Forensics and Incident Response teams are available 24x7x365 at 1-800-993-8937 if you suspect or are experiencing a network incident of any kind.

For more information, please contact our team at **cybersecurity@schneiderdowns.com** or visit **www.schneiderdowns.com/cybersecurity**.