

# Has the Changing Cybersecurity Landscape Killed Backups?

Ben Nowacky // SVP Product, Axcient

## Threats are Escalating



### The New York Times

#### *Hundreds of Businesses, From Sweden to U.S., Affected by Cyberattack*

In Sweden, a grocery chain temporarily closed its doors after the attack. Some companies have been asked for \$5 million in ransom.



HELPNET  
SECURITY

**SMBs increasingly  
vulnerable to ransomware,  
despite the perception they  
are too small to target**

## SMBs in the US are in the crosshairs



**300x** more likely to  
be targeted than other  
industries

**25%** of all cyber  
attacks on finance were  
on US companies

**15%** of people successfully phished  
will be phished again within 1 year

**\$18.5m** avg cost of a  
cyber incident to US financial  
services company

**70%** of financial firms  
have experienced a security  
incident in last 12 months



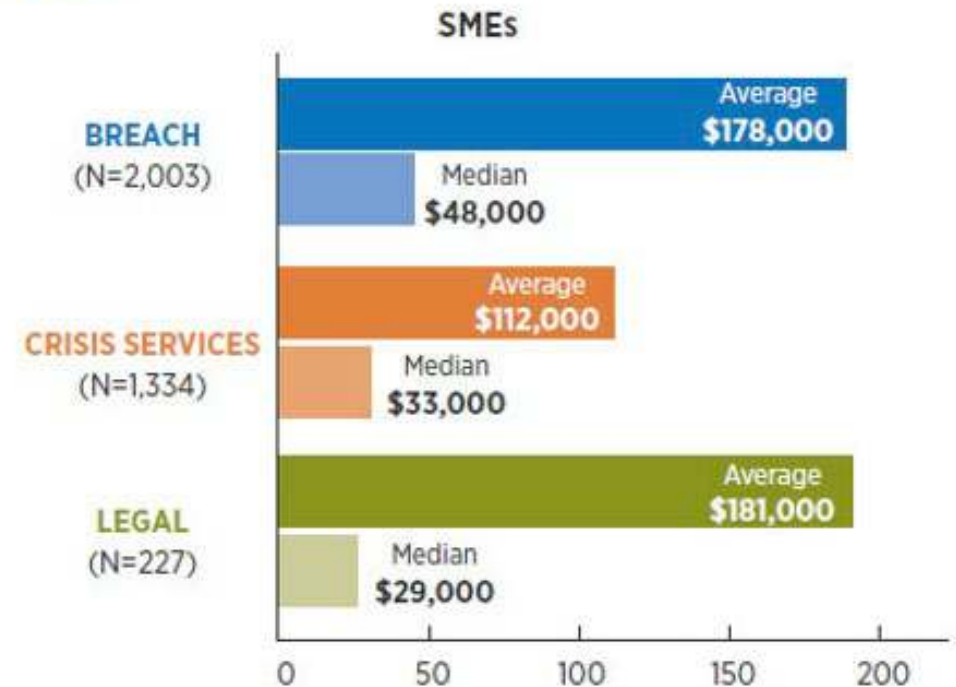
Sources: Webroot, 2021 Threat Report; CSO, Why are SMBs Under Attack by Ransomware, 2021; InfoSecurity, Most Ransomware Victims Are Hit Again After Paying, 2021

Higher Risk = Higher Insurance Rates



## AIG is reducing cyber insurance limits as cost of coverage soars

### Costs



Source: NetDiligence 2019 Cyber Claims Report

## Even the US Government Knows...

“OCIE has also observed an apparent increase in sophistication of ransomware attacks on SEC registrants. The perpetrators behind these attacks typically demand compensation (ransom) to maintain the integrity and/or confidentiality of customer data or for the return of control over registrant systems

In light of these threats, OCIE encourages registrants, as well as other financial services market participants, to **monitor the cybersecurity alerts published by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA..”**



...And they want it to stop!

“OFAC may impose civil penalties for sanctions violations based on **strict liability**, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC... **Enforcement responses range from non-public responses, including issuing a No Action Letter or a Cautionary Letter, to public responses, such as civil monetary penalties.**



And It's Not Just the Initial Attack

# FORTUNE

**The FBI broke up a Russian hacker plot to extort millions from Tesla**






# What are they after

- The most pressing attacks are often targeted at payment mechanisms (SWIFT or others) for the immediate pay-off
- Secondary attacks may result in data corruption, downtime, service disruption or general instability
- Data exfiltration is the long-tail and potentially the most dangerous

## A closer look at cyberattacks

The actors behind these incidents include not only increasingly daring criminals but also states and state-sponsored groups, with diverse goals and motivations.

THREAT ACTOR	MOTIVATIONS	GOALS	EXAMPLES
 <b>Nation-states, state-sponsored groups</b>	Geopolitical, ideological	Disruption, destruction, damage, theft, espionage, financial gain	Permanent data corruption, targeted physical damage, power grid disruption, payment system disruption, fraudulent transfers, espionage
 <b>Cybercriminals</b>	Enrichment	Theft/financial gain	Cash theft, fraudulent transfers, credential theft
 <b>Terrorist groups, hacktivists, insider threats</b>	Ideological, discontent	Disruption	Leaks, defamation, distributed denial-of-service attacks

**Source:** European Systemic Risk Board. 2020. "Systemic Cyber Risk."  
[https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219\\_systemiccyberrisk~101a09685e.en.pdf](https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf)



It's not a single solution...

NIST

## IDENTIFY

Asset Management  
Governance  
Risk Assessment  
Risk Management Strategy

## PROTECT

Access Control  
Awareness and Training  
Data Security  
Info Protection  
Process & Procedure  
Maintenance And Updates  
Protective Technology

## DETECT

Anomaly & Event Detection  
Continuous Security Monitoring  
Detection and Identification Process

## RESPOND

Incident Response Planning  
Communication  
Incident Analysis  
Mitigation  
Improvements / Post Mortem

## RECOVER

Recovery Planning  
Business Continuity Improvements  
Communication

Axcient



## Patchwork of mandates and requirements



---

### FINRA

4370. Business Continuity Plans and Emergency Contact Information

### PCIDSS

12.10.1 IR plan should address recovery and continuity

### SOX

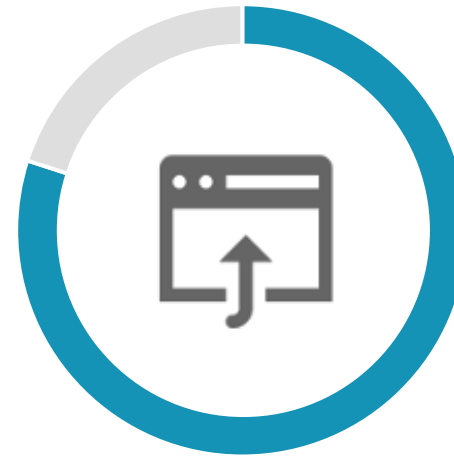
404 The responsibility of management for establishing and maintaining adequate controls...

# Backup is Failing Against these Pressures



**41%**

of organizations  
report inadequate  
backup and failure  
to meet SLAs

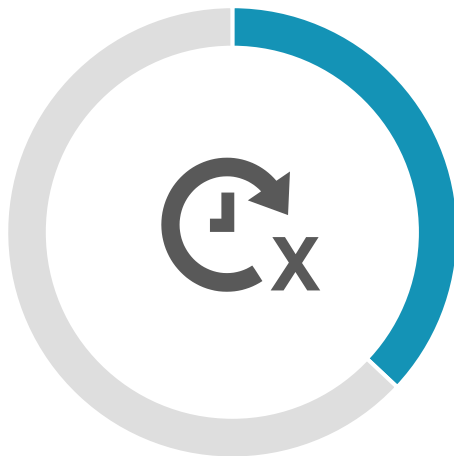


**80%**

of organizations say  
they are gapped  
between their ability  
to recover vs their  
need to recover

Source: Veeam, 2021 Data Protection Report, 2021

# Really, Really Failing



**37%**

of all backup  
jobs fail



**34%**

of all restore  
jobs fail



**58%**

Failure of  
recovery

Source: Veeam, 2021 Data Protection Report, 2021

## What If?



### Endpoint Backup

Protect data for remote employees and satellite offices



### No-Appliance BDR

Basic server backup to disk and cloud. Full business continuity



### Turn-Key BDR

Backup to turn-key appliance and cloud. Full business continuity



### Public Cloud Backup

Protect servers in Azure, AWS, Google with long-term retention



# Axcient

Axcient

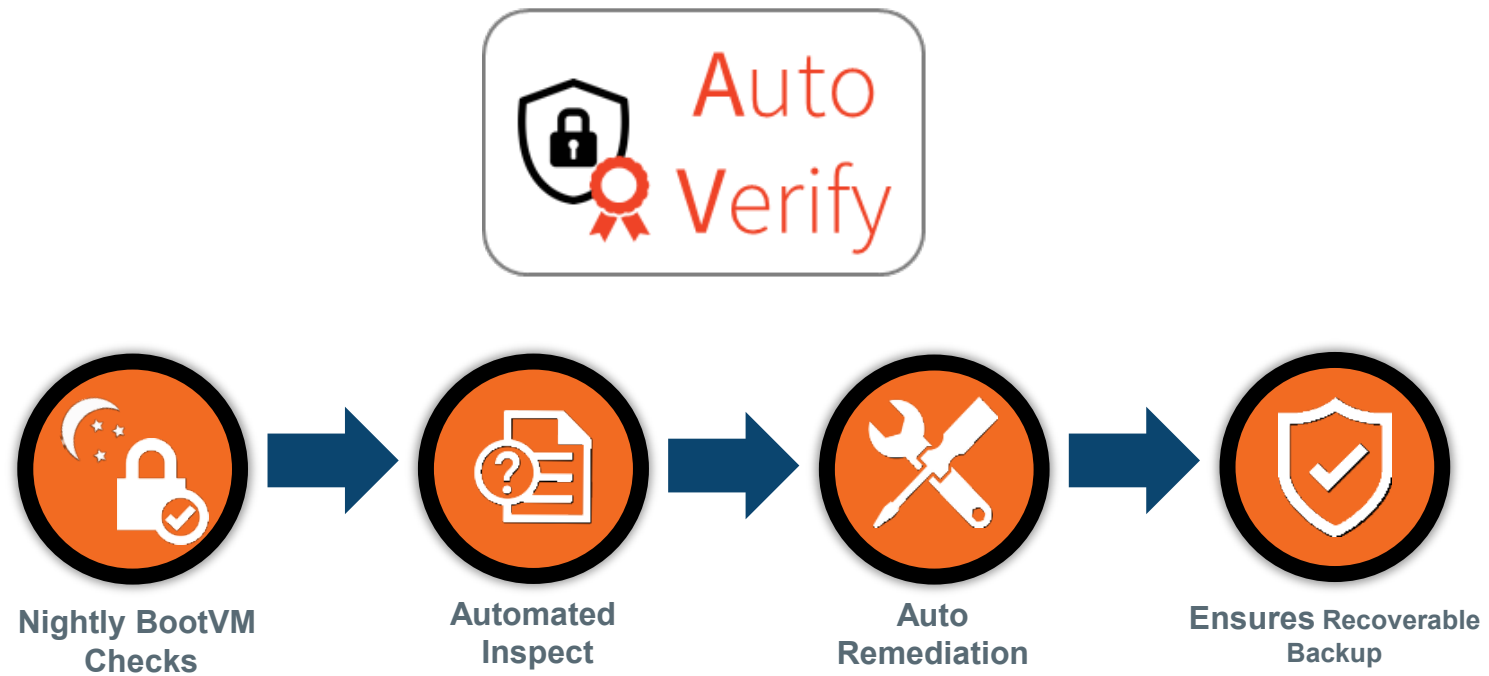
# Are my backups safe?



## AirGap in action – actual support ticket extract

- May 13<sup>th</sup> at 10:10am
- Partner: “Someone penetrated our system last night and managed to delete protected systems in multiple appliances.”
- May 13<sup>th</sup> at 10:31am (20-minutes later)
- Axcient: “Backups and protected servers on first appliance successfully recovered, we have 6 more to go.”
- May 13<sup>th</sup> at 1:58pm (4-hours later)
- Axcient: “All protected systems on all appliances were successfully recovered. Root and admin passwords changed.”
- May 15<sup>th</sup> at 3:26pm (2-days later)
- Axcient: “Kindly let me know if we can close this ticket.”
- May 15<sup>th</sup> at 3:32pm
- Partner: “Yes you can close it, thank you very much.”

But are the backups usable?



Questions?





# CURE DATA LOSS

Keep business running.