# Better Without Betterment

KIVU

# Better Without Betterment

Every day, Kivu engages with clients recovering from devastating ransomware attacks. Usually, that entails discussing a client's recovery needs with its insurer to determine whether recovery can be reimbursed.

As anyone who has worked with cyber insurance can attest, the concept of "betterment" can be a tricky minefield to negotiate successfully. When insureds are not communicating with their carriers, misunderstandings can leave policy-holders responsible for tens or hundreds of thousands of dollars in recovery expenses that they thought would be covered by their insurance policy but were excluded by a "betterment" clause. Organizations should know the right approach that will recover their systems and maximize recovery.

## What is "Betterment?"

Betterment is an insurance term that refers to the improvement of an asset after some alteration has been made. In general, insurance is intended to cover losses by "making you whole," but should not result in the policyholder reaping gain. To illustrate this, consider a three-bedroom home lost in a fire. Homeowners' insurance would surely cover the replacement cost of the house. However, it wouldn't pay for constructing a larger four-bedroom home to replace the original home. The expansion of the replacement home would be "betterment" versus the initially insured home, so the homeowner would be responsible for covering the incremental cost of construction to build the bigger house.

## Why is Betterment Confusing for Cyber Insurance?

For recovering computer systems, the concept of betterment gets a bit murky. Cyber insurance policies include a strict prohibition on betterment. Insurance carriers intend to support restoring policyholders' technology environments to the state they were in before an incident occurred. Ultimately, that could also increase risk and the potential for future losses. The state that an environment was in before an incident included one or more conditions that were the root causes of the incident. So, putting a policyholder's systems back exactly the way they were before could enable the same incident to occur again!

In practice, no insurance carrier requires a policyholder to put things back exactly as they were. In some cases, this isn't even possible when organizations are using long-deprecated hardware or software that can't be restored after a damaging ransomware attack. So, organizations must collaborate with service providers and their insurance carriers to develop a clear course of action for recovery that will restore functionality cost-effectively while also reducing cyber risk.

KIVU

## How Do We Avoid Betterment?

Unfortunately, no insurance carrier offers clear and concise guidelines to define "betterment." In practice, however, carriers find some commonality:

| Example Service From Recovery Provider | Is it Betterment? | Explanation |
|---|---|---|
| Support to restore data from backups | Definitely no | A provider lending support to restore data from backups shortens a period of business interruption and doesn't result in any net-new or improved technology capability. |
| Support to install and configure software (e.g., to rebuild a server or reimage a workstation) | Probably no | Service providers may perform patching and configuration changes to reduce vulnerabilities in newly installed software. While the restored systems might be better from a risk perspective, they're fundamentally the same systems. As long as changes don't result in incremental labor costs, there likely won't be an issue. |
| Procure and implement new systems to replace *existing systems* that were impacted by an incident. | Maybe | Insurance carriers closely scrutinize hardware purchases and won't support them without a strong financial rationale. Policyholders need to make a case that new purchases were more cost effective than repairing the old system. |
| Procure and implement net-new systems to restore a business-critical *capability* that was impacted by an incident | Maybe | Unlike the prior scenario, this claim focuses on the capability provided by the underlying systems rather than the systems themselves.<br>In some cases, restoring a capability using old technology may cost more than buying new technology to deliver the same capability. An organization restoring its email system might buy new mobile devices instead of continuing to use older devices that are declining in the market. |
| Upgrade deprecated software with newer versions | Probably yes | Organizations often want to take the opportunity to restore damaged systems with newer or better software than what they had before. While insurance carriers typically won't cover the cost of the updated software licenses, the labor cost to install updated software might be acceptable provided it doesn't exceed the cost to reinstall the old software. |
| Procure and implement new security technology to provide enhanced resilience to future attacks | Definitely yes | Any net-new security capability that wasn't in the environment before an incident would be considered betterment by most insurance carriers. Insurance simply will not pay to deploy a new multi-factor authentication solution or email security tool as part of the necessary cost of recovery from an incident even if it results in reduced risk for the insured. |

A close read of these scenarios, all of which are commonly encountered in ransomware recovery, yields two takeaways. First, while the purchase of software and hardware is almost always considered betterment, services (i.e., labor costs) usually aren't even when they result in identifiable improvements to an organization's technology environment. Second, insurance carriers are laser-focused on identifying and supporting the most cost-effective path to recovery. Thus, even recovery paths that result in significant improvements to the organization's risk profile or operational capabilities can be acceptable provided there isn't any incremental expense compared to other options.

## Recover Fast, Recover Strong

When recovering from ransomware, organizations tend to focus on minimizing downtime. However, IT outages also present an unexpected opportunity to make needed changes to the technology environment without creating additional disruption. While no one wants a cyber event, activating a cyber insurance policy can enable organizations to tap outside support and expertise that would not otherwise be available to them. When clients use the right expertise to remediate cyber events, they can leverage the incident to help prevent future incidents. An experienced incident responder can also help organizations leverage the resources used to recover and prevent future incidents.

Changes that should be considered as part of a recovery effort are those that enhance resilience against future attacks such as:

- **Implementation of cyber hygiene.** While the team may not have identified the root cause of its incident at the time when a recovery is occurring, most security incidents tend to result from a few common deficiencies in cyber hygiene. The US government regularly updates a list of the top routinely exploited vulnerabilities[1] , and the Center for Internet Security (CIS) maintain a list of the top 20 most critical IT security controls.[2] If cyber hygiene is lacking in the environment, consider deploying it now.

- **Upgrading of systems underpinning business-critical services.** The fact that insurance may not pay for an upgrade doesn't mean the organization shouldn't. When systems are already down and need significant maintenance, it might be the right time to upgrade operating system software, databases, and other business applications.

- **Modernization of select services.** If the team has been mulling a migration to the cloud for key functions (e.g., email, file storage and sharing, backups, etc.), this might be the right opportunity. With many cloud migration tasks now automated by software from the cloud providers themselves, the cost to move key services like email to a cloud-based platform might be reimbursable because it will be less than restoring corresponding on-prem infrastructure.

- **Consult, collaborate, communicate.** Like everyone else, insurance carriers want to understand what they are paying for. Often, the most critical element for recovery is communication. An ongoing and open conversation between the insurance carrier, counsel, the recovery experts and the policyholder (i.e. the organization that suffered the incident) can identify questionable expenses early and potentially justify the costs. And, in cases where a projected expense won't be covered, timely communication also enables the policyholder to identify an alternative approach.

## Looking Forward

Identifying and analyzing opportunities to recover stronger during a stressful cyber incident seems overwhelming, but this is where outside support really shines. Organizations should lean heavily on the knowledge and expertise of industry leaders to help prioritize changes that will reduce the likelihood of future attacks.

---

1. *https://www.cisa.gov/uscert/ncas/alerts/aa21-209a*
2. *https://www.cisecurity.org/controls*

Contact us to learn more at
info@kivuconsulting.com

Kivu is a leading global cybersecurity firm dedicated to offering best-in-class cybersecurity services. Since 2009, Kivu has been providing a full suite of services covering the entire incident lifecycle, specializing in the forensic response to cyberattacks and ransomware incidents.

If you are experiencing a suspected active data incident, contact us at **incidentresponse@kivuconsulting.com** or call **+1 855.548.8767 (United States)** or **+44 203.997.8334 (Europe).**

KIVU