

# NetSafe

Keep On Caring™

## Cybersecurity Alert

Introducing  
**CyberCrisis Vault**


A crucial layer of assurance to access patient information during a cyber crisis

### Healthcare Cyberattack & Breach Epidemic

#### Statistics That Give Pause


#### Healthcare is under attack by hackers

**32,000** intrusion attacks  
per day, **2X >** financial and retail  
  
FortiGuard Labs


**89%** breached  
in the past 2 years  
  
Ponemon

#### And is falling behind in securing information systems against risk

**54%** risk assessment grade,  
down **18%**  
  
Tenable Network Security

**9th** in overall security  
as compared to other industries  
  
Security Scorecard

#### Hospitals highly vulnerable to Ransomware with the threat growing rapidly

**88%**  
**of ALL**  
Ransomware attacks  
occur in healthcare  
  
Solutionary, an NTT Group

**350%**  
annual growth of  
Ransomware attacks  
  
Cisco

**4X**  
Ransomware attacks on  
healthcare will quadruple by  
2020  
  
CSO Online

#### The consequences to hospital revenue and reputation are sobering

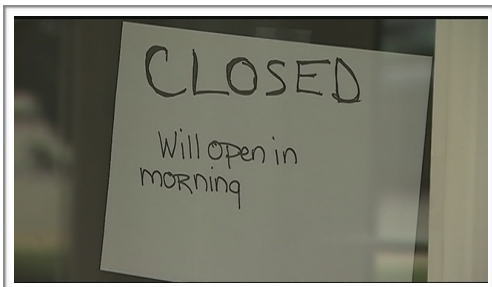
 **\$3 million** average loss to reputation, abnormal turnover  
of patients, increased patient acquisition activities, and diminished goodwill

## Why Healthcare, Why Now?

Hackers have found rich and fertile ground in healthcare. During the next few years, experts expect for the frequency and success of cyberattacks on healthcare to grow by more than 500%. Here's why:

1. Healthcare has more valuable data, in larger volumes than other industries
2. Healthcare networks and systems have inherent gaps and vulnerabilities caused by:
  - a. The increased demand for medical record access by patients and providers
  - b. The increased merger of disparate hospital information systems
  - c. The difficulty in detecting identity fraud is much harder in the medical field than, for example, the financial industry where sophisticated fraud alert services have been built
  - d. The complexity of trying to assemble information from multiple sources and systems
  - e. Human error
3. The relative infancy of healthcare cybersecurity preparedness and prioritization
4. Hackers are succeeding and getting paid well

Hackers seek the path of least resistance, and the healthcare industry has shown a willingness to pay these blackmail demands. When hit with ransomware, many hospitals have desperately paid the ransom in order to get the medication and other records required to provide critical care to patients.



## Unique Challenges of Ransomware, Malware & Breaches

We have seen and heard from many customers how NetSafe can enable continuity of care by providing access to patient information on local workstations at the point-of-care when host systems become unavailable. **However, these serious and growing cyber threats pose unique challenges which cannot be met by traditional contingency plans. They demand a new level of crisis management preparedness to ensure your facility's on-going operation.**

Downtimes caused by cyberattacks are a new challenge because they lock down your IT infrastructure beyond your control, in the case of ransomware. They can also force you to shut down systems hospital-wide to prevent further exposure of patient information. This means electronic information is unavailable and failsafe backups and redundancy solutions will need to be checked for infection before they can be used again. When hospital-wide systems are locked down during a cyberattack, there is no information access...**anywhere**...and the time to restoration is uncertain, if not impossible.

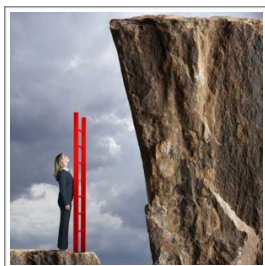


Meanwhile, your staff requires this electronic information to do their jobs. Imagine their workflows disrupted by the chaos of a cyberattack lock down. How will they manage:

- Medication administration and verification
- Finding patient history, lab results, radiology and others...
- Critical care departments, such as stroke and trauma
- Admissions and processing of arriving patients
- Access to forms and administrative information
- Other scenarios...

In fact, the lack of availability threatens patient safety, hospital revenue, increases potential liability, and may even impact your reputation.

In any of these cases, you will not have the protection of your local NetSafe information to maintain operations while your systems undergo the prolonged validation and restoration required following these attacks.



Your IT team will be focused on bringing systems back and protecting privacy, while clinicians will be pleading for their patient's information. As one hospital IT Director stated of their ransomware cyberattack experience lacking patient information, "Without a plan you are standing at a cliff."

***"Without a plan you are standing at a cliff."***

Anonymous Hospital IT Director

## Mistaking Resiliency for Crisis Management

When we discuss the first response challenges to accessing patient information at the earliest stage of a cyber crisis, many hospitals think that they are already protected. **They are mistaken.**

Traditional redundancy and distributed resiliency solutions such as server farms, remote data centers, virtualization and cloud storage may be important components, but in a cyberattack, they may also be compromised and unavailable for access when the crisis first occurs. Before they can be used again, they will need to be checked for infection. At a minimum, it will take several hours, if not several days to restore hospital-wide systems.

A crisis management solution commonly referred to as an Emergency Response Plan (ERP) or Breach Response Process must ensure that a hospital has an immediate response for continuing patient care.

## Enter NetSafe CyberCrisis Vault

Interbit Data has recognized the urgency of the information access required in these cyber crisis situations. This is why we created NetSafe CyberCrisis Vault. We have taken our best practice NetSafe technology and designed a separate, patent-pending deployment which removes it from the threats of network infections, while providing near access to the information clinicians and administrative staff need to respond to the crisis.

The Vault is an all-inclusive hardware, software, and monitoring solution that makes it easy for hospitals to acquire, implement and maintain. As experts in downtime, Interbit Data has done the work, so you don't have to.

### NETSAFE SOFTWARE, HARDWARE VAULT



**Patent Pending**  
Isolation — Restrictions  
Security — Redundancy

### STREAMLINED IMPLEMENTATION



### HOSPITAL PREPARATION & READINESS



### REMOTE MANAGEMENT & SUPPORT BY INTER-



## Hospital Reputation Management Protected

While hospitals are protected by their insurance from some of the potential liability and fines from accidents, mistakes and privacy breaches, this is of little solace. The greater threat is to a hospital's reputation and, ultimately, the financial impact that rating may entail. Perhaps the greatest risk, then, is from the public's perception of the hospital's ability to protect patient safety during and in the aftermath of an event.

Putting a Crisis Management Emergency Response Plan in place with components like our NetSafe CyberCrisis Vault solution, will go a long way towards maintaining a hospital's reputation during and after an incident. **A hospital which can ensure positive patient experiences in the face of an attack or breach will be thought of much more highly than one which has to divert admissions, has slow clinician response times, experiences challenges continuing patient care, or in the worst case, makes mistakes that endanger a patient's life.**

Social media is a common place for patients and the public to comment about breach and cyberattack incidents. There have been many social media posts where patients, and even staff, have complained vehemently about the "unacceptable" lack of access to patient information to clinicians, staff and others in the care network. Hospitals are much more likely to receive praise from the public in these posts when patient care is maintained, even when patient privacy is breached.

## Making It Easy for NetSafe Customers

Good news! Your hospital has already implemented the NetSafe software application with your EHR system. Adding the extra layer of support provided by Cyber Crisis Vault is simple. Interbit provides the hardware, software, and support.

As an existing NetSafe customer, purchasing the CyberCrisis Vault is also affordable. The new platform — including hardware, software, setup, remote monitoring and support — may cost less than \$500 a month — **a minimal investment for a significant reduction in risk.**

## About Interbit Data, Inc.

Interbit Data provides software automation solutions that ensure clinicians and hospital staff always have easy, secure and reliable access to patient information whenever and wherever they need it, so they can get back to their patients and *Stay In Touch*. Our products integrate with any EHR platform and HCIS to distribute reports to help care teams stay informed. We are the pioneer and best practice leader in downtime business continuity providing reliable access to patient information at the point-of-care during downtimes, as well as during more challenging cyber crises.

Using our software automation solutions, hospitals can be more efficient, streamline workflows and improve overall patient safety while elevating the level of care. Our 750+ worldwide customers are a testament to their indispensable value.

For more information, visit [interbitdata.com](https://interbitdata.com)