NAS insurance

Cyber Liability

State-of-the-art Insurance
Coverage and Support Services

Cyber. Evolved.

Our most expansive cyber insurance update ever.

Our 2018 NetGuard® Plus cyber liability insurance policy has been reengineered to help businesses of all sizes combat cybercrime and address emerging cyber risks.

With our broadest coverage yet, the NAS cyber liability insurance solution is an effective combination of great coverage, state-of-the-art risk mitigation services, and unparalleled support from our in-house claims experts.

Highlights of our cutting edge NetGuard® Plus cyber liability policy include:

- Free Pre-breach Expert Consultation
- $0 Retention for initial legal advice regarding a security/privacy incident
- Additional Defense Costs Limit Built into the Policy
- Telephone Consumer Protection Act (TCPA) Defense Coverage
- Dependent System Failure Coverage Built into the Policy
- Reward Expenses for informants providing information about a cyber incident
- Separate Breach Event Costs Limit Enhancement Built into the Policy
- Post-breach Remediation Costs

NetGuard® Plus now includes an industry-leading System Failure coverage component, with expanded coverage for data recovery and a period of restoration of up to 6 months.

Preventative Services

Being insured isn't always the same as being prepared. So we now offer our cyber policyholders a range of discounted proactive services from leading cybersecurity experts.

Services include:

- Network Security Assessments
- Table-top Incident Readiness Consulting
- Security Awareness Training
- Email Phishing Simulations
- PCI Compliance Reviews

NAS Insurance is a Lloyd's of London coverholder and benefits from Lloyd's of London's financial strength and robust capitalization.

Lloyd's reliability is reflected in its financial ratings:
AM Best: A (Excellent) Class XV
Standard & Poor's: A+ (Strong)

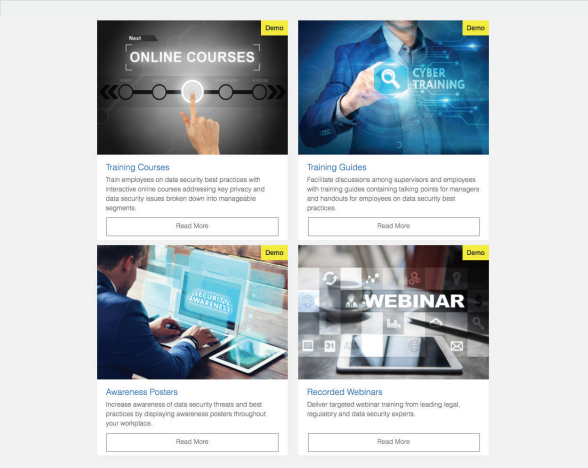
NAS cyberNET®

Online Support and Risk Management

As an NAS cyber liability insurance policyholder, your policy includes **NAS CyberNET®**, giving you access to expert cyber risk advisors when you need them, plus 24/7 online training courses, sample policies, vendor agreement templates and more.

NAS CyberNET® helps you and your organization mitigate the risk and impact of a cyber breach.

- Cyber Security Training
- Compliance Material
- Risk Management



Web-based training and support

Expert Cyber Claims Handling

Our cyber claims team provides rapid response support for your clients. We handle over 1,000 cyber claims each year and with more than 20 in-house cyber claims team members, NAS provides expert service and support when your clients need it most.

Working in close coordination with nationally-recognized privacy & security experts, the NAS claims team is at your side every step of the way.

- Expert “Breach Coach” and legal counsel services
- IT security and forensic experts
- Public relations/advertising support
- Breach notification
- Call center and website support
- Credit monitoring and identity theft restoration services

Industry Leading Expertise

Cyber Breach Response Network

Our team of incident response experts are leaders in the field and are here to help you. We have the experience and know-how to respond quickly and get your business back on track.

The following is a partial list of experts with whom we are proud to collaborate:

Wilson Elser · Kroll · Lewis Brisbois · Navigant · epiq Systems · Kivu · Mullen Coughlin · jackson lewis (All we do is work.) · McDonald Hopkins (A business advisory and advocacy law firm®) · Crypsis

Description of Coverage

Multimedia Liability – Duty to defend coverage for third party claims alleging liability resulting from the dissemination of online or offline media material, including claims alleging copyright/trademark infringement, libel, slander, plagiarism or personal injury.

Security and Privacy Liability – Duty to defend coverage for third party claims alleging liability resulting from a security breach or privacy breach, including failure to safeguard electronic or non-electronic confidential information or failure to prevent virus attacks, denial of service attacks or the transmission of malicious code from an insured computer system to the computer system of a third party.

Privacy Regulatory Defense and Penalties - Duty to defend coverage for regulatory fines and penalties and/or regulatory compensatory awards incurred in privacy regulatory proceedings/investigations brought by federal, state, local, or foreign governmental agencies, such as proceedings/investigations alleging HIPAA violations.

PCI DSS Liability - Duty to defend coverage for assessments, fines, or penalties imposed by banks or credit card companies due to non-compliance with the Payment Card Industry Data Security Standard (PCI DSS) or payment card company rules.

NEW! TCPA Defense - Coverage for the defense of claims alleging violation of the Telephone Consumer Protection Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the CAN-Spam Act, or any similar federal, state, local or foreign law regulating the use of telephonic or electronic communications for solicitation purposes.

Breach Event Costs – Coverage for reasonable and necessary mitigation costs and expenses incurred as a result of a privacy breach, security breach or adverse media report, such as legal expenses, proactive and reactive public relations expenses, IT forensic expenses, breach notification costs (including voluntary notification costs), and the cost to set up call centers and provide credit monitoring and identity theft assistance.

NEW! Post Breach Remediation Costs – Coverage for post-breach remediation costs incurred to mitigate the potential of a future security breach or privacy breach. ($25,000 Sublimit)

BrandGuard® - Coverage for loss of net profit incurred as a direct result of an adverse media report or notification to affected individuals following a security breach or privacy breach.

System Failure – Coverage for (1) reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen and (2) business income loss and interruption expenses incurred due to an unplanned outage, interruption, failure, suspension, or degradation of service of an insured computer system, including any such incident caused by a hacking attack.

NEW! Dependent System Failure – Coverage for (1) reasonable and necessary amounts incurred to recover and/or replace electronic data that is compromised, damaged, lost, erased, corrupted or stolen and (2) business income loss and extra expenses incurred due to an unplanned outage, interruption, failure, suspension, or degradation of service of a service provider computer system that is caused by specified cyber perils, including a denial of service attack, malicious code, and acts of cyber terrorism.

Cyber Extortion – Coverage for extortion expenses incurred and extortion monies paid as a direct result of a credible cyber extortion threat.

Cyber Crime – Coverage for (1) loss of money or securities incurred due to financial fraud, including wire transfer fraud; (2) charges incurred for unauthorized calls resulting from fraudulent use of an insured telephone system; and (3) your loss of money, securities, or other property due to phishing attacks, expenses incurred to notify customers of phishing attacks directed against you, and the cost of reimbursing customers or clients for their losses that result from phishing attacks against you.

NEW! Reward Expenses – Coverage for reasonable amounts paid to an informant for information not otherwise available, which leads to the arrest and conviction of a person or group responsible for a privacy breach, security breach, system failure, cyber extortion threat, financial fraud, telecommunications fraud, or phishing attack. ($50,000 Sublimit)

NEW! Court Attendance Costs – Coverage for reasonable costs incurred to attend court, arbitration, mediation, or other legal proceedings or hearings as a witness in a claim covered under the policy. (Daily maximum limit of $500.00, subject to overall aggregate limit of $25,000)