FREQUENTLY ASKED QUESTIONS – PALADIN RISK REPORTS

TO: U.S. RETAIL INSURANCE AGENTS & BROKERS
FROM: STEVE ROBINSON, NATIONAL CYBER PRACTICE LEADER
RE: FAQ – PALADIN CYBER RISK REPORTS WITH NEW AND RENEWAL QUOTES ON RPSSmallBusiness.com
DATE: 08/10/22

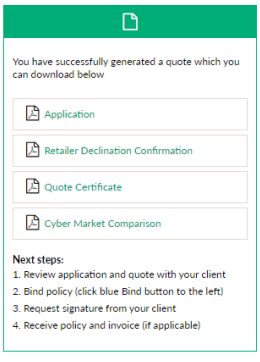
We are pleased to announce a new value-added benefit provided by BCS, Lloyd's and Hiscox to insureds at no cost on the RPSSmallBusiness.com platform. Paladin Shield can help insureds prevent cyberattacks that can disrupt their business and affect their bottom line. For BCS, Lloyd's and Hiscox new business and renewal quotes, Paladin Cyber will run a scan of publicly available data detailing your insured's internet-facing network infrastructure and configuration settings, and provide the findings in an easy-to-understand risk report. These carriers have partnered with Paladin Cyber to provide this valuable insight into your insured's information security posture before their next renewal (or, along with their new business quote), identifying potential vulnerabilities in their defenses against serious cyber threats such as ransomware, business email compromise and other forms of unauthorized access into their IT systems.

The Paladin risk report will help your insured identify critical vulnerabilities such as unpatched software, open remote access ports (which are known to be a leading attack vector for ransomware attacks), weaknesses in email defenses, and more. Sharing this report with your insured will not only help them bolster their defenses against costly attacks, it will also help secure the most favorable terms and pricing for their cyber insurance. Risk management conversations like these help agents increase their value to their clients and improve retention rates as well. We have created an FAQ to help guide you through the process.

- **Who is Paladin Cyber?**
  Paladin Cyber provides a full-stack cybersecurity platform to arm companies and their insurers in the fight against cybercrime. Combining proactive inbox and browser protection with employee training and visibility into a company's cyber risk through continuous monitoring, Paladin helps organizations stop costly attacks before they occur. Insureds that activate and engage with Paladin have been shown to be 50% less likely to file a cyber claim.

- **What is a Paladin risk report?**
  A Paladin risk report is an easy-to-understand, moment-in-time assessment of an organization's vulnerabilities to certain cyber threats. The report identifies specific, actionable measures a business can take in the areas of remote access, outbound email protection, website security, exposed data and host vulnerabilities to significantly improve their information security posture.

- **Where do I find the report?**
  The report can be found in the documents section on the quote screen in RPSSmallBusiness.com (to the right, in the same area where the quote certificate is found). Click the link to download the pdf report.



- **Which carriers on the RPSSmallBusiness.com platform utilize Paladin to provide risk reports?**
  Currently, BCS, Lloyd's and Hiscox partner with Paladin Cyber to provide their risk reports to insureds. CFC utilizes separate, proprietary technology to conduct scans that are incorporated into their underwriting process in real-time.

NOTE: Certain of our carriers have contracted with Paladin Cyber (Paladin) to run network scan risk reports for potential insureds when providing quotes. The results of Paladin risk reports are based on the website URL provided in the cyber insurance application. Please validate the accuracy of this address with your insured as it will affect the results of the report. The relationship between Paladin and each insurer is a separate contractual relationship, not affiliated with Risk Placement Services (RPS). RPS does not endorse the vendor, warrant the results, or verify the accuracy of information contained in risk reports. Information found in risk reports does not constitute an offer of insurance coverage. RPS is not qualified to and does not offer information security recommendations or advice. Insureds should consult information security experts for advice of this nature. Specific questions about results found in a Paladin risk report can be directed (regardless of which insurer has issued the report) to Paladin Cyber via email at contact@meetpaladin.com or via phone at 800-418-8593.

- **Is this Paladin scanning process an intrusion into my insured's system, website or network?**
  No. Paladin Cyber scans an organization's internet-facing network infrastructure. This information is publically available, and is the first place hackers look when assessing an attack opportunity.

- **Does permission need to be given to run this scan?**
  Because information obtained in the Paladin risk report is publically available based on the company's web domain, and does not involve any intrusion into a network, permission is not required to run the scan.

- **How should I share this report with my insured? Doesn't it contain confidential information?**
  While the report identifies vulnerabilities within an organization's information security posture, the information gathered in the report is publicly available. For that reason, any vulnerabilities identified in the report are able to be identified by cyber criminals that are utilizing similar scan technology. No hacker would learn anything by intercepting this email that they could not readily find out on their own. Retail agents who are concerned about communicating this content via email may want to send this report to your insured in an encrypted format.

- **I'm not an IT expert, how will I explain the report to my client? What if they have questions about the findings?**
  Your insured can set up a vulnerability consultation with a Paladin security expert by booking time at this link: https://calendly.com/critical-vuln-consultation/vulnerability-consultation. In addition, every Paladin risk report has a "Chat" icon and contact information for your insured to reach out to Paladin directly with questions and they stand ready to assist with answers. RPS is not qualified to provide information security advice to retail agents or their insureds.

- **What if the results of the scan are "bad"? Will they impact my insured's ability to bind their quote?**
  Currently, the Paladin risk reports do not tie directly to automated underwriting decisions for any carriers on the RPSSmallBusiness.com platform. This could change in the future, and decisions of this nature could vary among insurers. However, for accounts that are referred off-platform, the results of the scan could factor into decisions concerning coverage availability, pricing, terms and conditions. Paladin risk reports should be shared with insureds and any vulnerabilities identified should be remedied or discussed with Paladin. It is always recommended that insureds register with Paladin Shield to ensure they receive the tools and updates necessary to increase their cyber resiliency.

- **What is Paladin Shield?**
  Paladin Shield secures an organization against ransomware and other common attacks by layering critical protections into one easy solution. Listed below are just a few of the key benefits of using Paladin Shield:

  1. **Help Employees Identify Dangerous Emails:**
     Inbox defender feature helps identify dangerous emails. Whether the insured checks mail on the web or use Outlook, they'll will be warned of potentially dangerous situations.

  2. **Block Dangerous Websites & Files:**
     Online Protection features automatically check websites before they load and block danger.

  3. **Train Employees to Identify Danger:**
     Cyber University helps build the insured's human firewall by turning their biggest vulnerability into their greatest asset. Resulting in an aware workforce that actively looks out for and reports new threats.

NOTE: Certain of our carriers have contracted with Paladin Cyber (Paladin) to run network scan risk reports for potential insureds when providing quotes. The results of Paladin risk reports are based on the website URL provided in the cyber insurance application. Please validate the accuracy of this address with your insured as it will affect the results of the report. The relationship between Paladin and each insurer is a separate contractual relationship, not affiliated with Risk Placement Services (RPS). RPS does not endorse the vendor, warrant the results, or verify the accuracy of information contained in risk reports. Information found in risk reports does not constitute an offer of insurance coverage. RPS is not qualified to and does not offer information security recommendations or advice. Insureds should consult information security experts for advice of this nature. Specific questions about results found in a Paladin risk report can be directed (regardless of which insurer has issued the report) to Paladin Cyber via email at contact@meetpaladin.com or via phone at 800-418-8593.

- **If the results of the Paladin risk report are "good", will my insured receive lower premiums?**
  At this time, Paladin risk report results do not inform underwriting decisions in automated quotes for the carriers who partner with Paladin on the RPSSmallBusiness.com platform. This could change in the future, creating a cause-and-effect relationship that aligns sound controls with coverage pricing, availability, terms and conditions.

- **The report doesn't contain all of the detailed information, where can the rest of the specific information referenced in the report be obtained?**
  Insureds can receive the full results of the report by registering with Paladin Shield, which is entirely free as an added benefit with their BCS, Lloyd's or Hiscox policy (Paladin typically costs $6,000/year per company). Instructions for this free and easy process are provided in the materials they receive with the Paladin risk report. There is an "Activate Shield" icon on the first page of the report. The insured can also set up a vulnerability consultation with a Paladin security expert to review their report by booking time at this link: https://calendly.com/critical-vuln-consultation/vulnerability-consultation.

- **Does my insured have to remedy any negative findings before their renewal (or before binding their new business quote) in order to get coverage?**
  It is highly recommended that insureds remedy all identified vulnerabilities identified within the Paladin risk report to help ensure the most sound information security practices for their organization. While the risk report results do not currently tie directly to underwriting decisions in the automated underwriting process for any of the carriers on the RPSSmallBusiness.com platform, this is subject to change at any time. For insureds whose new or renewal quotes are referred off-platform, underwriters from the various insurers may require remediation before agreeing to provide terms. Each carrier will make those determinations in alignment with their respective underwriting criteria.

- **Does my insured have to register for Paladin Shield in order to continue their coverage with their carrier?**
  Not at this time, but this is subject to change. In fact, we expect it will change in the future. If offered by their carrier, it is highly recommended that insureds register for Paladin Shield to receive regular updates on new vulnerabilities as they develop, and, for access to the free tools for inbox and browser protection, in addition to user education provided by Paladin Shield.

- **Is there a cost for the insured to use the Paladin Shield Service?**
  No. The cost of Paladin Shield is paid for by the insurance carriers who partner with Paladin Cyber. This includes all software protections, security awareness trainings, and security consultations provided by Paladin, which is a benefit of $6,000/year per company based on Paladin's rates.

- **Can we get the report without the insured signing up for Paladin Shield?**
  Yes, but not the complete report. Insureds who wish to access all of the detailed remediation suggestions found within a Paladin risk report must register with Paladin Shield.

- **What are the next steps after the insured contacts Paladin to activate their Shield?**
  Installation of Paladin Shield takes minutes and can be done with the assistance of Paladin Cyber over the phone. The insured can set up one administrator account to activate their Paladin Shield account. To add employees, the administrator simply registers employee names and email addresses, and employees get access to personalized portals. All protections can be installed in three clicks.