Your Policyholders Demand Instant Access to Their Data. **Is It Protected?**

Cybersecurity Expert Discusses Comprehensive Approach for Insurers

In this tight marketplace, survival depends on business agility and cost savings — on using cloud technologies to launch new products and services and self-service portals and mobile apps to retain and attract agents and policyholders.

Today's agents and customers are savvier and more demanding than ever before. They want instant access to their information over the Web and their mobile devices. They expect to complete transactions on the spot by connecting to an insurer's back-end systems.

As a result, a growing number of companies are integrating their existing systems and business processes with Web portals, third-party vendors, cloud-based applications and mobile technologies — not fully aware of the cyber threats that await them.

"By opening up data to external channels, insurers are exposing customer records and sensitive company information to an unprecedented level of threats in cyberspace," said Bryant G. Tow, director of Commercial Cybersecurity, CSC. "And many insurers that have already been infiltrated don't even know it."

Insurers Face New Cyber Threats

Tow notes that it wasn't long ago that insurers felt secure if their perimeter was secure — when user name and password technologies were keeping unwanted visitors out of internal systems.

But as they deploy new technologies, their security concerns go well beyond protecting internal systems. They extend all the way to cyberspace.

"There are a number of new questions CIOs need to be asking," says Tow. "What would happen if a sophisticated adversary breached customer records and released them to the public? What if an agent's laptop or mobile device containing confidential data about pricing strategies was stolen and ended up in the wrong hands? What if costly disruptions and thefts hurt their bottom line?"

Embarrassing public breaches could tarnish an insurer's brand and strangle new business. Such disruptions could invite shareholder wrath. Confidential data that ended up in the wrong hands could significantly hurt competitiveness. A number of large financial services firms have already fallen victim to cyber attacks, and nearly every breach of customer data has become a national headline.

In the new era of openness, Tow explains, cybersecurity is no longer a mere compliance matter or the "cost of doing business." It is one of the primary business imperatives that both life and property and casualty insurers must address.

Needed: Holistic Approach

Now that data is no longer contained within the perimeter, protecting the perimeter will no longer suffice.

Insurers need a new, proactive strategy that embeds information security into the heart of their global business processes and operations, and secures company data wherever it may reside.

As part of a more proactive strategy, insurers must assess their cybersecurity strengths and weaknesses and design an enterprise solution that secures their people, facilities, processes and technology — lock, stock and barrel.

Insurers must also identify, prioritize and manage risk relative to its potential impact on mission-critical operations — so they can balance security needs against cost considerations, business success plans and the need to maintain organizational agility.

Cybersecurity programs must provide real-time visibility into processes, systems, data and equipment — a complete view of any vulnerabilities that may arise across the enterprise — and arm insurers with the tools, operational resources, procedures and managed cybersecurity services they need to "prevent, detect, recover and revise."

> "By opening up policyholder data to external channels, insurers are exposing customer records and sensitive company information to an unprecedented level of threats in cyberspace. And many insurers that have already been infiltrated don't even know it."
>
> Bryant G. Tow,
> Director of Commercial Cybersecurity,
> CSC

CSC: Insurance Cybersecurity Leader

Drawing on more than 50 years of global outsourcing experience, CSC has secured business processes, systems and sensitive data for the world's largest and most demanding government and commercial organizations.

"We bring a holistic approach to identity management, compliance and business continuity/disaster recovery, as well as a full range of cybersecurity services that extend from the development of corporate and mission strategy down to the very bits and bytes that make up the billions of threats our global security centers monitor daily," Tow said.

For instance, CSC's Security Stack offering provides a strategy for responding to a natural catastrophe or other disasters with a proactive four-layer response model that incorporates crisis management, situational awareness, business continuity and disaster recovery planning.

"We offer extensive experience designing, managing and securing the mission-critical data of the world's leading insurers," he added. "We intimately understand the broad new threats insurers face and the steps they must take to eliminate them."

CSC

Learn more about CSC's cybersecurity solutions at www.csc.com/cybersecurity

Your Policyholders Demand Instant Access to Their Data. **Is It Protected?**

Cybersecurity Expert Discusses Comprehensive Approach for Insurers

In this tight marketplace, survival depends on business agility and cost savings — on using cloud technologies to launch new products and services and self-service portals and mobile apps to retain and attract agents and policyholders.

Today's agents and customers are savvier and more demanding than ever before. They want instant access to their information over the Web and their mobile devices. They expect to complete transactions on the spot by connecting to an insurer's back-end systems.

As a result, a growing number of companies are integrating their existing systems and business processes with Web portals, third-party vendors, cloud-based applications and mobile technologies — not fully aware of the cyber threats that await them.

"By opening up data to external channels, insurers are exposing customer records and sensitive company information to an unprecedented level of threats in cyberspace," said Bryant G. Tow, director of Commercial Cybersecurity, CSC. "And many insurers that have already been infiltrated don't even know it."

Insurers Face New Cyber Threats

Tow notes that it wasn't long ago that insurers felt secure if their perimeter was secure — when user name and password technologies were keeping unwanted visitors out of internal systems.

But as they deploy new technologies, their security concerns go well beyond protecting internal systems. They extend all the way to cyberspace.

"There are a number of new questions CIOs need to be asking," says Tow. "What would happen if a sophisticated adversary breached customer records and released them to the public? What if an agent's laptop or mobile device containing confidential data about pricing strategies was stolen and ended up in the wrong hands? What if costly disruptions and thefts hurt their bottom line?"

Embarrassing public breaches could tarnish an insurer's brand and strangle new business. Such disruptions could invite shareholder wrath. Confidential data that ended up in the wrong hands could significantly hurt competitiveness. A number of large financial services firms have already fallen victim to cyber attacks, and nearly every breach of customer data has become a national headline.

"By opening up policyholder data to external channels, insurers are exposing customer records and sensitive company information to an unprecedented level of threats in cyberspace. And many insurers that have already been infiltrated don't even know it."

Bryant G. Tow,
Director of Commercial Cybersecurity,
CSC

In the new era of openness, Tow explains, cybersecurity is no longer a mere compliance matter or the "cost of doing business." It is one of the primary business imperatives that both life and property and casualty insurers must address.

Needed: Holistic Approach

Now that data is no longer contained within the perimeter, protecting the perimeter will no longer suffice.

Insurers need a new, proactive strategy that embeds information security into the heart of their global business processes and operations, and secures company data wherever it may reside.

As part of a more proactive strategy, insurers must assess their cybersecurity strengths and weaknesses and design an enterprise solution that secures their people, facilities, processes and technology — lock, stock and barrel.

Insurers must also identify, prioritize and manage risk relative to its potential impact on mission-critical operations — so they can balance security needs against cost considerations, business success plans and the need to maintain organizational agility.

Cybersecurity programs must provide real-time visibility into processes, systems, data and equipment — a complete view of any vulnerabilities that may arise across the enterprise — and arm insurers with the tools, operational resources, procedures and managed cybersecurity services they need to "prevent, detect, recover and revise."

CSC: Insurance Cybersecurity Leader

Drawing on more than 50 years of global outsourcing experience, CSC has secured business processes, systems and sensitive data for the world's largest and most demanding government and commercial organizations.

"We bring a holistic approach to identity management, compliance and business continuity/disaster recovery, as well as a full range of cybersecurity services that extend from the development of corporate and mission strategy down to the very bits and bytes that make up the billions of threats our global security centers monitor daily," Tow said.

For instance, CSC's Security Stack offering provides a strategy for responding to a natural catastrophe or other disasters with a proactive four-layer response model that incorporates crisis management, situational awareness, business continuity and disaster recovery planning.

"We offer extensive experience designing, managing and securing the mission-critical data of the world's leading insurers," he added. "We intimately understand the broad new threats insurers face and the steps they must take to eliminate them."

CSC

Learn more about CSC's cybersecurity solutions at www.csc.com/cybersecurity

Your Policyholders Demand Instant Access to Their Data. **Is It Protected?**

Cybersecurity Expert Discusses Comprehensive Approach for Insurers

In this tight marketplace, survival depends on business agility and cost savings — on using cloud technologies to launch new products and services and self-service portals and mobile apps to retain and attract agents and policyholders.

Today's agents and customers are savvier and more demanding than ever before. They want instant access to their information over the Web and their mobile devices. They expect to complete transactions on the spot by connecting to an insurer's back-end systems.

As a result, a growing number of companies are integrating their existing systems and business processes with Web portals, third-party vendors, cloud-based applications and mobile technologies — not fully aware of the cyber threats that await them.

"By opening up data to external channels, insurers are exposing customer records and sensitive company information to an unprecedented level of threats in cyberspace," said Bryant G. Tow, director of Commercial Cybersecurity, CSC. "And many insurers that have already been infiltrated don't even know it."

Insurers Face New Cyber Threats

Tow notes that it wasn't long ago that insurers felt secure if their perimeter was secure — when user name and password technologies were keeping unwanted visitors out of internal systems.

But as they deploy new technologies, their security concerns go well beyond protecting internal systems. They extend all the way to cyberspace.

"There are a number of new questions CIOs need to be asking," says Tow. "What would happen if a sophisticated adversary breached customer records and released them to the public? What if an agent's laptop or mobile device containing confidential data about pricing strategies was stolen and ended up in the wrong hands? What if costly disruptions and thefts hurt their bottom line?"

Embarrassing public breaches could tarnish an insurer's brand and strangle new business. Such disruptions could invite shareholder wrath. Confidential data that ended up in the wrong hands could significantly hurt competitiveness. A number of large financial services firms have already fallen victim to cyber attacks, and nearly every breach of customer data has become a national headline.

"By opening up policyholder data to external channels, insurers are exposing customer records and sensitive company information to an unprecedented level of threats in cyberspace. And many insurers that have already been infiltrated don't even know it."

Bryant G. Tow,
Director of Commercial Cybersecurity,
CSC

In the new era of openness, Tow explains, cybersecurity is no longer a mere compliance matter or the "cost of doing business." It is one of the primary business imperatives that both life and property and casualty insurers must address.

Needed: Holistic Approach

Now that data is no longer contained within the perimeter, protecting the perimeter will no longer suffice.

Insurers need a new, proactive strategy that embeds information security into the heart of their global business processes and operations, and secures company data wherever it may reside.

As part of a more proactive strategy, insurers must assess their cybersecurity strengths and weaknesses and design an enterprise solution that secures their people, facilities, processes and technology — lock, stock and barrel.

Insurers must also identify, prioritize and manage risk relative to its potential impact on mission-critical operations — so they can balance security needs against cost considerations, business success plans and the need to maintain organizational agility.

Cybersecurity programs must provide real-time visibility into processes, systems, data and equipment — a complete view of any vulnerabilities that may arise across the enterprise — and arm insurers with the tools, operational resources, procedures and managed cybersecurity services they need to "prevent, detect, recover and revise."

CSC: Insurance Cybersecurity Leader

Drawing on more than 50 years of global outsourcing experience, CSC has secured business processes, systems and sensitive data for the world's largest and most demanding government and commercial organizations.

"We bring a holistic approach to identity management, compliance and business continuity/disaster recovery, as well as a full range of cybersecurity services that extend from the development of corporate and mission strategy down to the very bits and bytes that make up the billions of threats our global security centers monitor daily," Tow said.

For instance, CSC's Security Stack offering provides a strategy for responding to a natural catastrophe or other disasters with a proactive four-layer response model that incorporates crisis management, situational awareness, business continuity and disaster recovery planning.

"We offer extensive experience designing, managing and securing the mission-critical data of the world's leading insurers," he added. "We intimately understand the broad new threats insurers face and the steps they must take to eliminate them."